BOARD OF SUPERVISORS
AGENDA LETTER

Clerk of the Board of Supervisors
105 E. Anapamu Street, Suite 407
Santa Barbara, CA 93101
(805) 568-2240

Agenda Number:

Department Name:	County Executive Office, and General Services
Department No.:	012, 063
For Agenda Of:	April 10, 2018
Placement:	Administrative
Estimated Time:	
Continued Item:	No
If Yes, date from:	
Vote Required:	Majority

TO:	Board of Supervisors	
FROM:	County Executive Office	Jeff Frapwell, Assistant County Executive Officer, (805) 568-3432
	General Services	Janette D. Pell, Director (805) 560-1011
	Contact Info:	Thomas Gresham, Assistant Director (805) 568-2606
SUBJECT:	**Allocate Job Classification of Chief Information Security Office (Enterprise Leader) to the County Executive Office; All Districts.**	

County Counsel Concurrence
As to form: Yes

Auditor-Controller Concurrence
As to form: Yes

Other Concurrence: HR
As to form: Yes

Recommended Actions:

That the Board of Supervisors consider the following recommendations:

a) Approve and authorize the Chair to allocate one (1) full-time equivalent (FTE) Enterprise Leader – General position effective April 23, 2018, funded by the Risk Management Fund in the County Executive Office (to be used and recruited for a Chief Information Security Officer); and

b) Determine pursuant to California Environmental Quality Act (CEQA) Guidelines Section 15378(b)(4) that the above action is a government fiscal activity which does not involve any commitment to any specific project which may result in a potentially significant physical impact on the environment, and therefore is not a project subject to environmental review.

Summary Text:

The County of Santa Barbara is in need of a Chief Information Security Officer (CISO) to lead an overall cybersecurity program that will manage the risk from growing cyber threats. This position is charged with building the best instrument to support the County's information security challenges from top to bottom, across all departments. The role is critical and vital in today's security landscape. The average total cost of a data breach globally was $3.62 million in 2017.

Background:

Cybersecurity risk is just one factor of the overall County business risk management strategy. Cybersecurity risk, like with all risks, cannot be entirely eliminated, but instead must be managed through informed decision making processes. The objective of a cybersecurity program is to reduce the probability and effect of a cyber-event to an organization's operations, assets, and individuals. The Chief Information Security Officer (CISO) is the individual tasked with the development and enforcement of a comprehensive cybersecurity program. A balanced, informed decision-making process concerning cyber risk management will lead to a positive effect on the business, operationally and financially.

The Countywide Information Technology Strategic Plan calls for the creation of a countywide security program to identify and manage information technology risks across the enterprise. The CISO position is identified as the key role to drive the vision and roadmap for the creation of a cybersecurity program. The cybersecurity program will focus on establishing, assessing and managing risk across all departments to provide greater visibility for senior management and collaboration to provide adequate protection of information and services. Attachment 2 provides the CISO job description.

As part of the County's cybersecurity program, the Chief Information Security Officer will fulfill the following duties:

- Security Vision & Strategy – The CISO is responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.
- Policy Guidance – The CISO will establish appropriate standards and controls, manage security technologies, and propose policies and procedures that safeguard information and ensure that due diligence is performed in alignment with regulatory requirements.
- Assessment – The CISO identifies programs and systems appropriate for assessment. Assessed risk is then presented to the department for acceptance or remediation.
- Response Planning – The CISO approves and conducts disaster recovery exercises, incident response, breach reporting and impact disclosures among other events.

The CISO will provide consistent leadership and guidance to County staff to assist in maturing cybersecurity capabilities in response to an increasing risk from cyber-attacks. Acting as the liaison to external agencies, the CISO will collaborate with federal and state partners to remain informed of new threats, vulnerabilities and other risks to the County.

The risk of having some type of cybersecurity breach is real. The 2017 calendar year saw some of the biggest cyber threats in recent history, with millions of consumers and thousands of businesses affected by attacks like WannaCry and Cryptolocker and/or incidents similar to the Equifax and Uber data breaches. Gartner reports that worldwide, information security spending exceeded $86.4 billion in 2017 and the 2017 Cybercrime Report anticipates cybercrime damages to cost the world $6 trillion annually by 2021. The 12th annual "Cost of Data Breach Study" sponsored by IBM Security and independently conducted by the Ponemon Institute, revealed that the average total cost of a data breach in 2017 was $3.62 million globally.

Our peers in the news in March 2017 include; the Colorado Department of Transportation who's ransomware attack (SamSam) left 2000 employees unable to work for multiple days and an estimated $1.5 million in response and remediation costs (still ongoing), the City of Atlanta was shut down for six days

following a ransomware attack for $51,000 bitcoin. The requested $51,000 in bitcoin ransom does not compare to the losses associated with a complete shutdown of government services. A 'mere' 10.8% phishing success rate forced Los Angeles County to notify approximately 756,000 individuals that their personal information may have been compromised. The attack occurred on May 13, 2016, when 1,000 County employees received phishing emails. Approximately 108 employees were successfully phished. "That information may have included first and last names, dates of birth, Social Security numbers, driver's license or state identification numbers, payment card information, bank account information, home addresses, phone numbers, and/or medical information, such as Medi-Cal or insurance carrier identification numbers, diagnosis, treatment history, or medical record numbers," said the County of Los Angeles Chief Executive Office.

Web browsing to compromised sites and/or phishing attacks has exposed the County to Cryptolocker, Petya, Wannacry, and other miscellaneous ransomware attacks in 2017, resulting in significant remediation and recovery efforts by Information Technology (IT) and end users. The total impact to the County is difficult to quantify as we don't have a Cybersecurity Program and departments aren't required to report a breach. In total, the massive WannaCry outbreak caused an estimated $1 billion in damage in just four days, according to Stu Sjouwerman, CEO at KnowBe4.

Last month in the County of Santa Barbara, there were approximately 3,000 confirmed malicious attacks on our infrastructure. This does not include port scans and other reconnaissance activities that attackers may be performing against our infrastructure in an attempt to find and exploit vulnerabilities blocked by another safeguard. If we included these reconnaissance activities the actual number is likely to be much greater than 3,000.

In the absence of security policies, security awareness training and staff development, asset management, risk and security controls, effective monitoring and reporting and timely incident response, any one of these attack vectors could be the source of a major system outage and/or a significant non-compliance financial penalty.

The County of Santa Barbara does carry Cyber Liability insurance. Cyber Liability insurance is designed to mitigate losses but it should not be used in place of robust preventative measures or implementation of security best practices. The key to a good cybersecurity program is prevention.

Fiscal and Facilities Impacts:

Budgeted: Yes

Fiscal Analysis:

Funding Sources	Current FY Cost:	Annualized On-going Cost:	Total One-Time Project Cost
General Fund			
State			
Federal			
Fees			
Risk Fund:		$ 195,000.00	
Total	$ -	$ 195,000.00	$ -

Narrative:
The position will be managed in the County Executive Office and funded in the Risk Management Division's budget, Fund 1912 – County Liability-Self Insurance Fund (Risk Fund).

The salary and benefits for an Enterprise Leader is estimated at $195,000 per year. If approved, it is anticipated that a recruitment will be initiated immediately with the position being filled to begin the 2018-19 Fiscal Year.

Staffing Impacts:

Legal Positions:	FTEs:
1.0	1.0

Special Instructions:

Please send one (1) copy of the minute order to Joseph Toney, Assistant Director, General Services and one (1) copy of the fully-executed resolution and minute order to Stefan Brewer, Position Control Division, Human Resources.

Attachments:

1. Salary Resolution
2. Chief Information Security Officer Job Description

Authored by:

Thomas Gresham, Assistant Director, General Services