County of San Mateo

Inter-Departmental Correspondence

Department: COUNTY MANAGER
File #: 19-970 Board Meeting Date: 10/8/2019

Special Notice / Hearing: None
Vote Required: Majority

To: Honorable Board of Supervisors

From: Michael P. Callagy, County Manager

Subject: Board of Supervisors' Response to the 2018-2019 Civil Grand Jury Report, "Security of Elections Announcements"

RECOMMENDATION:
Approve the Board of Supervisors' response to the 2018-2019 Civil Grand Jury Report, "Security of Elections Announcements."

BACKGROUND:
On July 24, 2019, the 2018-2019 San Mateo County Civil Grand Jury issued a report titled "Security of Elections Announcements." The Board of Supervisors is required to submit comments on the findings and recommendations pertaining to the matters over which it has some decision-making authority within 90 days. The Board's response to the report is due to the Honorable Donald J. Ayoob no later than October 22, 2019.

DISCUSSION:
The Grand Jury made 17 findings and 14 recommendations in its report. The Board responses follow each finding and recommendation that the Grand Jury requested that the Board respond to within 90 days.

FINDINGS

Vulnerability of Public Trust in Election Communications

Finding 1:
The veracity of the County's election broadcasts on any ACRE or CMO online communication platform is important to the public's trust in the electoral process.

Response
Agree

Finding 2:

Unlike DHS, ACRE does not include the security of online election communications when describing election security on its website.

Response:
ACRE submitted a response to this Finding directly to the Civil Grand Jury.

Finding 3:
Protecting online communication platforms with multi-factor authentication that is susceptible to SIM hijacking, phishing, and man-in-the-middle attacks-as is the case with the use of one-time PINs (OTPs) sent to cell phones-exposes the County to election disinformation attacks.

Response:
Partially agree. SIM hijacking is a complex form of mobile phone fraud. ISD recommends that only County-issued devices be used to manage Election and Social Media information. The mobile carriers that provide the County with mobile device service have procedures in place to protect County accounts and devices from these types of attacks. Additionally, the County uses a multi-factor security solution that provides phishing and Real-Time Man-in-the-Middle (MITM) resistance.

Vulnerability of the County's Email

Finding 4:
Although the County implemented several email security protections that provide many of the DMARC benefits following a 2016 phishing attack, the County's email security practices do not follow DHS guidelines for federal agencies due to the absence of complementing DMARC protection.

Response:
Partially agree. In 2017, DHS issued binding operational directive (18-01) requiring that all federal agencies enhance email security by enabling an additional security policy, called Domain-based Message Authentication, Reporting, and Conformance (DMARC), with the primary goal of making it difficult to successfully spoof government services. The DHS directive does not directly apply to local governments or the County. However, ISD has already implemented portions of this recommendation and will continue to enhance email security over time using this and other protocols as general guidance for email security best practices.

Finding 5:
The County utilizes multi-factor authentication methods for its email that remain susceptible to SIM hijacking, phishing, and man-in-the-middle attacks.

Response
Partially disagree. According to security and telecommunication experts, SIM hijacking is a complex form of mobile phone fraud. The County uses an industry leading secure multi-factor solution that with capabilities that provide phishing and Real-Time Man-in-the-Middle (MITM) resistance because the technology relies on the physical device and not the SIM/phone number.

Vulnerability of ACRE's Website

Finding 6:
ACRE's website security practices do not follow DHS guidelines for federal agencies requiring the use of multi-factor authentication protection by users who have the system permissions to alter the ACRE webpages.

Response:
ACRE submitted a response to this Finding directly to the Civil Grand Jury.

Finding 7:
ACRE outsource the domain management and hosting of its smcacre.org website to a third-party vendor.

Response:
ACRE submitted a response to this Finding directly to the Civil Grand Jury.

Vulnerability of Social Media Accounts

Finding 8:
The San Mateo County Information Security Training produced by ISD does not make any recommendations for security practices of official County social media accounts.

Response:
Partially agree. All County staff are required to take annual IT security training. While there is no specialized security training related to social media accounts, the IT security training provided to staff does provide basic IT security training instruction that is also applicable to social media applications. ISD will include more specific examples of social media IT security in next year's training.

Finding 9:
The San Mateo County Departmental Social Media Policy produced by CMO requires that multiple employees share official social media account passwords.

Response
Agree. ISD will work with CMO to update this policy and submit it to the Board of Directors for approval by November 30, 2019.

Finding 10:
ACRE and CMO employee share passwords to their official social media accounts listed in Table 1 with multiple employees within their offices.

Response:
Agree

Finding 11:
The San Mateo County Departmental Social Media Policy produced by CMO does not make any recommendations about using multi-factor authentication to protect against an unlawful takeover of social media accounts.

Response:
Agree. The County Social Media Policy will be updated by November 30, 2019.

Finding 12:
The ACRE and CMO social media accounts listed in Table 1, with the exception of the CMO Facebook page, do not use multi-factor authentication.

Response
Agree. Not all social media solution providers currently support multi-factor authentication.

Status of Cyber Hygiene

Finding 13:
ACRE and ISD could strengthen their coordination of the evaluation and addition of security features to address election security.

Response
Partially disagree. ACRE and ISD meet and discuss all aspects of cybersecurity at monthly IT Security meetings and quarterly IT Governance meetings. Additional coordination meetings occur on an as needed based on projects or events.

Finding 14:
ISD utilizes a DHS "Vulnerability Scanning" service for the entire County, but ACRE does not utilize any of the other seven free elections-specific DHS services listed in Table 2.

Response
Partially disagree. ISD uses services and information provided through DHS, MS-ISAC, EI-ISAC, as well as NCRIC to protect County resources. The County currently subscribes to at least one service listed in Table 2 and is in the process of evaluating additional services. ISD is responsible for the overall cybersecurity administration of the County, and as such it would not be appropriate for any individual Department to unilaterally utilize additional services without ISD's involvement and coordination. ISD will meet with ACRE to determine if additional security tools or services are needed and will implement them based on the confirmed business needs and benefits.

Finding 15:
ISD runs network vulnerability assessments ("Vulnerability Scanning") for the County devices but does not audit the practices of employees to identify behavioral sources of network vulnerability.

Response:
Agree. ISD audits and investigates issues within the County's environment but has not yet implemented a County-wide network User behavior analytics (UBA) solution. ISD is currently investigating products with UBA capabilities to determine which solutions would best meet the needs of the County.

Finding 16:
The Internal Audit Division of the County Controller's Office "performs internal audits of departments' operations," which has sometimes included cyber hygiene assessments.

Response:
The Controller's Office submitted a response to this Finding directly to the Civil Grand Jury.

Finding 17:
The Internal Audit Division of the County Controller's Office has not performed a cyber hygiene assessment of the Elections Division of ACRE.

Response:

The Controller's Office submitted a response to this Finding directly to the Civil Grand Jury.

RECOMMENDATIONS

Protect the Public Trust in Election Communication

Recommendation 1:
Incorporate Communications into Election Security Definition: ACRE should adopt a policy that defines election security to include the security of the ACRE website, ACRE staff email accounts, social media accounts used for ACRE announcements, and other platforms ACRE uses for publishing election announcements. ACRE should implement this recommendation by December 31, 2019.

Response:
ACRE submitted a response to this Recommendation directly to the Civil Grand Jury.

Recommendation 2:
Publish Updated Security Policy: ACRE should update the ACRE website's written descriptions of the election security to incorporate the policy resulting from R1 on the security of election communications in addition to the current focus on security of (a) registration, (b) vote casting, and (c) results tabulation. ACRE should implement this recommendation by June 30, 2020.

Response:
ACRE submitted a response to this Recommendation directly to the Civil Grand Jury.

Protect the County's Email

Recommendation 3:
Prevent Spoofing with DMARC: ISD, CMO, and ACRE should improve email security for employees involved in election announcements and should at least partially implement the Recommendation by June 30, 2020.

Response
ACRE, ISD, and CMO will collaborate to improve email security for employees involved in election announcement and have partial implementation by June 30, 2020.

Recommendation 4:
Combat ACRE Email Account Phishing with FIDO Keys: ACRE should provide FIDO physical security keys to each of its permanent elections employees and require the use of those FIDO keys as part of their multi-factor authentication for accessing their County email accounts. ACRE should implement this recommendation by December 31, 2019.

Response
The Recommendation requires technical analysis by ISD, which will be completed by December 31, 2019. ACRE and ISD will collaborate to determine the best means to implement FIDO type MFA for Elections Division's email accounts. ISD will determine which U2F devices (FIDO Keys) are best able to secure County systems and provide them as needed to ACRE and other County Departments.

Recommendation 5:
Combat Other Email Account Phishing with FIDO Keys: ACRE should identify County employees

outside of ACRE that have a role in election announcements (e.g., Chief Communications Officer, senior ISD employees, etc.) and ask that the departments of the identified employees provide FIDO physical security keys to each of the identified employees and require the use of those FIDO keys as part of their multi-factor authentication for accessing their County email accounts. ACRE should complete this recommendation by December 31, 2019.

Response
ACRE submitted a response to this Recommendation directly to the Civil Grand Jury.

The Recommendation requires technical analysis by ISD, which will be completed by December 2019. ISD will determine which U2F devices (FIDO Keys) are best able to secure County systems and provide them as needed to ACRE and other County Departments.

Protect ACRE's Website

Recommendation 6:
Combat Website Account Phishing with FIDO Keys: ACRE should require all County employees whose user accounts allow them to alter the ACRE website to use FIDO physical security keys as part of their multi-factor authentication. ACRE should implement this recommendation by December 31, 2019.

Response
ISD will work with ACRE to implement the Recommendation, which requires technical analysis by ISD, that will be completed by December 31, 2019. ISD will determine which U2F devices (FIDO Keys) are best able to secure County systems and provide them as needed to ACRE and other County Departments.

Recommendation 7:
Combat Island Hopping with FIDO Key Vendor Requirement: ACRE and ISD should require employees and contractors of any vendor that hosts the ACRE website to use FIDO physical security keys as part of their multi-factor authentication. ACRE and ISD should implement this recommendation by December 31, 2019.

Response
ACRE submitted a response to this Recommendation directly to the Civil Grand Jury.

The Recommendation requires technical analysis by ISD, which will be completed by December 31, 2019. ISD will determine which U2F devices (FIDO Keys) are best able to secure County systems and provide them as needed to ACRE and other County Departments.

Protect the Social Media Accounts

Recommendation 8:
Stop Sharing Social Media Account Passwords: ACRE and CMO should implement procedures whereby communications staff manage official County social media accounts with multi-user administration, and no employees share social media account passwords. ACRE and CMO should implement this recommendation by October 31, 2019.

Response:
ACRE and CMO will collaborate to determine the best means to restrict social media account password sharing. In the meantime, ACRE has implemented a Team's feature for Twitter which allows multiple people to share an account without having to share a password.

Recommendation 9:
Request FIDO Key Feature If Not Available: ACRE and CMO should jointly draft and send a FIDO-key feature request citing this report to the social media companies used by the County to broadcast election announcements, but that do not currently offer FIDO account security protections-especially Instagram and Nextdoor. ACRE and CMO should implement this recommendation by August 31, 2019.

Response
This Recommendation has already been implemented. ACRE, ISD, and CMO collaborated on a letter sent to social media companies requesting that they confirm, or create, support for MFA and FIDO-key integration for their platforms.

Recommendation 10:
Combat ACRE Social Media Account Phishing with FIDO Keys: ACRE should require any employee social media accounts capable of administering the official ACRE social media pages listed in Table 1 to use FIDO physical security keys as part of their multi-factor authentication. ACRE should implement this recommendation by December 31, 2019.

Response
The Recommendation requires technical analysis by ISD, which will be completed by December 31, 2019. ISD will determine which U2F devices (FIDO Keys) are best able to secure County systems and provide them as needed to ACRE and other County Departments.

Recommendation 11:
Combat SMC Social Media Account Phishing with FIDO Keys: CMO should require any employee social media accounts capable of administering the official San Mateo County social media pages listed in Table 1 to use FIDO physical security keys as part of their multi-factor authentication. CMO should implement this recommendation by December 31, 2019.

Response:
The Recommendation requires technical analysis by ISD, which will be completed by December 2019. ISD will determine which U2F devices (FIDO Keys) are best able to secure Social Media sites and provide them as requested by County Departments.

<u>Improve Cyber Hygiene</u>
Recommendation 12:
Coordinate Election Security with Interdepartmental Working Group: ACRE and ISD should create an election security working group that meets periodically and is responsible for evaluating and improving the security of elections (a) registration, (b) vote casting, (c) results tabulation, and (d) communication within San Mateo County. ACRE and ISD should implement this recommendation by December 31, 2019.

Response:
The Recommendation has already been implemented.

Recommendation 13:
Evaluate Free DHS Elections Security Assistance Programs: ACRE and ISD election-security working group should evaluate the benefits of having all members of the election-security working group participate in any of the free DHS elections security assistance programs listed in Table 2.

ACRE and ISD should implement this recommendation by February 3, 2020.

Response
ACRE and ISD will collaborate to determine if any of the additional free services offered by DHS, beyond those already in use, would provide improved benefits. This assessment of DHS free services will be completed by October 30, 2019.

Recommendation 14:
Offer Behavioral Cyber Hygiene Audits: ISD and the County Controller's Office should develop a behavioral auditing program consisting of sampling the day-to-day routines and security practices of employees, contractors, and/or vendors and offer to audit each department within the County periodically to (1) evaluate compliance with existing cyber hygiene policies and (2) provide proactive advice on cyber hygiene improvements that could inform new policies. ISD and the Controller's Office should begin to implement this recommendation by offering to audit ACRE and ISD (itself) in time to finish by February 3, 2020.

Response:
The Recommendation requires further analysis. ISD in the process of reviewing and testing products with network and account User Behavioral Analytics (UBA) capabilities to determine which service or product would best meet the needs of the County. This analysis and testing will be completed by December 31, 2019.

SHARED VISION 2025:
Acceptance of the report contributes to the Shared Vision 2025 outcome of a Collaborative Community by ensuring that all Grand Jury findings and recommendations are thoroughly reviewed by the appropriate County departments and that, when appropriate, process improvements are made to improve the quality and efficiency of services provided to the public and other agencies.

FISCAL IMPACT:
Additional tools and services will be needed to implement the recommendations outlined above. ISD will provide the CMO with an estimate of ISD staff costs, consultants/contractors, and hardware/software by December 2019.