CONTRA COSTA COUNTY CIVIL GRAND JURY
REPORT NO. 2104

"Cyber Attack Preparedness in Contra Costa County"

RESPONSES TO FINDINGS:

F1. County IT Departments are chronically understaffed.

F1 response. The respondent agrees with the finding.

F2. Obsolete equipment poses a vulnerability threat to County Information Technology Security.

F2 response. The respondent agrees with the finding.

F3. Some County Information Technology Departments do not have time to conduct software and hardware updates, and vulnerability scans which are critical for cyber security because of understaffing.

F3 response. The respondent agrees with the finding.

F4. Some County departments with small Information Technology staffs do not have specialized cyber security personnel.

F4 response. The respondent agrees with the finding.

F5. Cyber security training is performed on an inconsistent basis in some County departments.

F5 response. The respondent agrees with the finding.

F6. County employees and contractors use personal storage devices (e.g., flash drives) on County computers.

F6 response. The respondent partially agrees with the finding.

Some County departments currently have technical controls which prohibit the use of personal storage devices on County computers.

F7. The use of personal devices makes County computers vulnerable to denial of service, data breaches or other cyber-attacks.

F7 response. The respondent agrees with the finding.

The industry is, however, moving in a direction where use of personal devices for some work functions is more common, and in some cases necessary.

F8. Information Technology expenditures and budgets in County departments are not transparently reported so it is difficult to identify redundant and duplicative Information Technology expenditures.

F8 response. The respondent agrees with the finding.

F9. Decentralized Information Technology structures increase vulnerability to cyber-attacks.

F9 response. The respondent agrees with the finding.

F10. The County's Information Technology structure is decentralized.

F10 response. The respondent partially agrees with the finding.

The County Administrator and Chief Information Officer have put into place an Information Technology Executive Advisory Committee, which will provide a centralized governance structure for Information Technology decisions.

F11. Based on interviews, Contra Costa County is at a disadvantage to hire Information Technology staff with cyber security expertise due to increased compensation and perks offered by some private enterprises.

F11 response. The respondent agrees with the finding.

RESPONSES TO RECOMMENDATIONS:

R1. The Board of Supervisors direct the County Chief Information Officer by December 2022 to create a talent pool within Department of Information Technology (DoIT) that includes cyber security experts to relieve chronic staffing shortages in all Information Technology departments.

R1 response. The respondent agrees with this recommendation.

Prioritization and timing of budget and staffing is, however, subject to approval. The Department of Information Technology (DoIT) has started addressing this by hiring a Chief Information Security Officer in 2020, and additional security staff whose focus are County-wide security efforts. This is in alignment with the County's Information Security Strategy.

R2. The Board of Supervisors direct the County Administrator by June 2022 to require all Information Technology departments to forbid use of personal devices on and with County computers (e.g., personal thumb drives).

R2 response. The respondent partially agrees with this recommendation.

The recommendation will be implemented, but documented exceptions may exist and be required due to departmental necessity.

R3. The Board of Supervisors direct the County Administrator by June 2022 to require the installation of software on all County computers that can scan for threats and viruses on any device attached to them.

R3 response. The respondent agrees with this recommendation.

The Chief Information Officer, Chief Information Security Officer, and Information Technology Executive Advisory Committee will work with County Administrator to adopt policy that requires this control. The Chief Information Officer and Chief Information Security Officer are additionally in process of ensuring the deployment of managed detection and response software on all county computers. This is in alignment with the County's Information Security Strategy.

R4. The Board of Supervisors direct the County Administrator by June 2022 to authorize DoIT to require system vulnerability testing on all County computer systems.

R4 response. The respondent agrees with this recommendation.

The Chief Information Officer, Chief Information Security Officer, and Information Technology Executive Advisory Committee will work with County Administrator to adopt policy that requires this control. Vulnerability testing is, and will continue to be, conducted on a risk basis. This is in alignment with the County's Information Security Strategy.

R5. The Board of Supervisors direct the County Administrator by June 2022 to require all county employees to complete annual cyber security awareness training.

R5 response. The respondent agrees with this recommendation.

The Chief Information Officer, Chief Information Security Officer, and Information Technology Executive Advisory Committee will work with County Administrator to adopt policy that requires this control. Additionally, the County is in the process of procuring security awareness training which will be administered jointly by DoIT, County Risk Management, and Human Resources. This is in alignment with the County's Information Security Strategy.

R6. The Board of Supervisors direct the County Administrator by June 2022 to have DoIT ensure mandatory updates are performed on all systems for all software applications.

R6 response. The respondent agrees with this recommendation.

The Chief Information Officer, Chief Information Security Officer, and Information Technology Executive Advisory Committee will work with County Administrator to adopt policy that requires this control. The County will adopt a vulnerability management policy which will ensure that mandatory updates are defined and communicated to all county departments, which is in alignment with the Information Security Strategy.

R7. The Board of Supervisors direct the County Administrator by December 2022 to have all County departments identify and replace obsolete Information Technology hardware.

R7 response. The respondent agrees with this recommendation.

The Chief Information Officer will work with relevant stakeholders to identify a methodology for identification and prioritization of replacement of obsolete hardware. Replacement will be conducted on a risk basis, and is contingent on departmental funding, staffing, and compliance obligations.

R8. The Board of Supervisors direct the County Administrator by June 2022 to require County departments to identify their planned IT spending in their overall budgets for transparency.

R8 response. The respondent agrees with this recommendation.

The County Administrator's Office works with each County department annually to develop the budget for the upcoming fiscal year and, as a part of that process, estimated interdepartmental charges from Information Technology and Telecommunications are reviewed. Additionally, non-County, Professional, Specialized Services (outside contracts), as well as minor equipment and fixed asset purchases are reviewed as part of the budget development process. Lastly, an annual amount of approximately $2 million in reserve funding is available for technology projects to be used to increase efficiencies and economies in Departments that do not have resources available within their normal operating budgets. Departmental requests for this funding include the name of the project, the amount of funding requested, a description of how the money will be spent, and any expected immediate and on-going benefit from the expenditure.