A REPORT BY

THE 2020-2021 CONTRA COSTA COUNTY CIVIL GRAND JURY

725 Court Street
Martinez, California 94553

Report 2104

Cyber Attack Preparedness In Contra Costa County

APPROVED BY THE GRAND JURY
Date 11-22-2021

SAMIL BERET
GRAND JURY FOREPERSON

APPROVED FOR FILING
Date 11/22/2021

JILL C. FANNIN
JUDGE OF THE SUPERIOR COURT

Contact: Samil Beret
Foreperson
(925) 608-2621

Contra Costa County Grand Jury Report 2104

Cyber Attack Preparedness in Contra Costa County

TO: Contra Costa County Board of Supervisors
Contra Costa County Department of Information Technology

SUMMARY

In the fall of 2019, hackers from the Balkans breached the Contra Costa County Library's (CCCL) Information Technology systems. The hackers obtained an administrative login, gained access to the network, took control, installed, and encrypted malicious software. In January 2020, the hackers demanded a ransom. This attack might have been prevented if the Library had cyber security software. Fortunately, the County's Department of IT (DoIT) was able to restore the Library's administrative systems within three days. However, the public system was inaccessible for two weeks at 29 locations, including library computers and all e-library features such as e-book delivery.

Contra Costa County uses IT as a foundation for data gathering, sharing, and storage throughout all county offices for essential services, including communication for law enforcement, healthcare, and infrastructure such as public works. Building and maintaining a robust IT environment require substantial capital outlays as well as annual expenditures.

The budget for DoIT in 2021 was $18.6 million, while the overall County budget is $4.06 billion. IT expenditures of individual County departments (e.g., Health Services, Sheriff's Office, and the Library) are not reflected in DoIT's budget since IT services are decentralized in various County departments. Further, those IT budgets for individual County departments are not separated from their overall budgets and therefore not transparent.

IT is subject to rapid evolution. New technologies are introduced weekly. Expensive hardware and software can quickly become obsolete or open to cyber-attack because older equipment might not support the necessary security upgrades.

Cyber-attacks are a threat to private and public institutions globally. According to cyber security experts, threats arise from disgruntled employees, foreign hackers or computer enthusiasts exhibiting their hacking abilities. Recent nation-wide breaches by external sources, including at SolarWinds, Colonial Pipeline, and Scripps, highlight the urgency to step up protection against attacks.

The Contra Costa County Library (CCCL), Contra Costa County Fire Protection District (Con Fire), and Contra Costa County Health Services Departments (Health Services) have experienced cyber-attacks. The Grand Jury investigated the general County IT landscape to determine vulnerabilities and plans to protect exposed systems and software.

The Grand Jury found that the overall County IT infrastructure is decentralized. Progress to eliminate redundancies (e.g., email systems, data storage) has been made since the 2017-2018 Grand Jury Report (1805). According to industry experts, decentralized organizations are less able to prevent cyber security breaches because they often lack key IT professionals, systems and/or coordination to deter cyber-attacks. The Grand Jury recommends that the County consider selective consolidation of IT services and resources into DoIT that will increase readiness to prevent and recover from cyber-attacks.

METHODOLOGY

The Grand Jury used the following investigative methods:

- Requests for information from County departments.
- Interviews with County IT department employees, County officials, and industry experts.
- Internet research of public, private, and government agency best practices.
- Review of news articles, including those exposing cyber-attacks, threats, and their outcomes.
- Review of prior Grand Jury Report 1805.
- Review of cyber security best practices based on National Institute of Security Technology, US Department of Homeland Security and California Office of Emergency Services.

BACKGROUND

In Contra Costa County, the IT infrastructure spans twenty-four County departments. The organization is headed by DoIT, the central IT group which coordinates the

individual departmental IT groups. DoIT is responsible for the central county computing complex, a county Wide Area Network, and numerous local area networks. Storage and backup procedures in this environment make data available on multiple devices via network servers or digital backups. DoIT is also responsible for the overall level of computing, printing, and telecommunications standards in the County. DoIT also provides business and technical consulting services to departments and managers throughout the County on a reimbursable basis.

In May 2018, the Grand Jury produced report 1805 on “Effectiveness of IT Operations in County Government.” Some of the Grand Jury recommendations were implemented while others were not. For example, the County’s IT Strategy and Disaster Recovery Plans have been updated. Recommendations not followed were due to the DoIT’s Chief Information Officer (CIO) not having the authority to mandate them due to the decentralized IT structure of the County. Specific examples include centralized procurement and installation of standard hardware and software on a County-wide basis.

The budget for DoIT in 2021 was $18.6 million, while the overall County budget is $4.06 billion. IT expenditures of individual County departments (e.g., Health Services, Sheriff’s Office, and the Library) are not reflected in DoIT’s budget. The Grand Jury reviewed the Comprehensive Annual Financial Report of the County and could not identify the IT budgets for individual county departments. It is difficult to determine precisely how much money the County is spending on IT and whether there are potential redundancies. This was a problem the previous Grand Jury Report 1805 identified.

Supplementing DoIT’s services, some large departments (e.g., Health Services Department, Sheriff’s Office) retain control over their own IT strategy, procurement, and routine IT services provided for their departments. These departments have their own data and network operations and dedicated IT staff. They have specialized requirements such as Health Insurance Portability and Accountability Act (HIPAA) compliance and the Sheriff’s Office’s use of Federal and State databases. Other smaller departments have small IT teams for local and/or specialized support, but generally rely on DoIT for procurement, equipment updates, and system maintenance. Based on the Grand Jury’s interviews, there is a lack of uniformity in systems and software, such as email systems and data storage.

Cyber-attacks pose a threat to governmental operations in Contra Costa County and nationwide. According to Check Point Software's Mid-Year Security Report, there were 93% more ransomware attacks in the first half of 2021 than in the same period last year. In addition, the attacks were marked by the rise of what is known as "Triple Extortion" ransomware. Not only is data encrypted, stolen, and moved, but if there is no response to the original threat for payment or the threat of a data leak, attackers may then launch a Denial-of-Service attack which locks up the targeted entity's system services to force it to the negotiation table. Cyber-attacks are increasing in their number and cost. IBM estimated that data breaches now cost companies $4.24 million per incident on average, with costs rising 10% compared to 2020.

> As the COVID-19 crisis spread globally, so did cyber attacks. The increase in virtual activities such as remote work and online shopping have made enterprise networks and popular websites a breeding ground for cybercrime. According to an advisory from the U.S. Department of Homeland Security Cyber Security and Infrastructure Agency (CISA) and the U.K.'s National Cyber Security Centre (NCSC), cybercriminals are targeting individuals, businesses, and organizations of all sizes with these attacks, including phishing attempts and trying to exploit security lapses in remote meetings. (https://www.gartner.com/en/human-resources/research/talentneuron/labor-market-trends/cybersecurity-labor-shortage-and-covid-19).

The 2019 Contra Costa County Library (CCCL) attack and subsequent disruption of e-Library Services heightened concern about county-wide cyber security. It demonstrated how a lack of cyber security experts in individual departments, and departmental cyber security oversight by DoIT, impact end users. Based on the Grand Jury's interviews, staff shortages intensify this problem. Small IT teams do not always have cyber security experts and are impacted if they have an open position or someone on leave. In this case, after the attack, DoIT took over the IT operations for the CCCL. DoIT provided resources including access to an external specialized team contracted to restore access to all systems. The estimated total costs were between $4 million and $6 million to upgrade firewalls, equipment and software updates or upgrades to bring the CCCL systems to industry standards. An insurance claim was filed for $1.2 million for recovery costs. The CCCL has applied for a State Library Association Technology Grant to upgrade its systems. If awarded, it will provide an additional $3 Million to bring the systems into compliance with current updated County standards.

> The routine software update may be one of the most familiar and least understood parts of our digital lives... Last spring, a Texas-based company called SolarWinds made one such software update available to its customers. It was supposed to provide the regular fare — bug fixes, performance enhancements — to the company's network management system... Hackers believed to be directed by the Russian intelligence service, the SVR, used that routine software update... as a vehicle for a massive cyberattack against America. (https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack).

Due to the SolarWinds Attack, software companies worldwide scrambled to update their software platforms to secure their systems. The Con Fire email servers were so obsolete that the Microsoft security patch to fix this vulnerability could not be applied in April 2021. When Con Fire's staff recognized the threat, they asked DoIT to assist. DoIT staff went on-site to perform hardware upgrades and expensive off-hours software updates. The total cost is still being assessed. While there was not a breach, Con Fire was vulnerable to one.

In 2018, the use of a flash drive by a contractor for the Contra Costa Health Services Department resulted in a data breach of patient medical information. This could have been prevented if adequate protocols were in place regarding the use of flash drives. (https://www.hipaajournal.com/contra-costa-health-plan-breach/)

DISCUSSION

The Grand Jury focused on three general areas that put the County at risk for a cyber-attack: 1) Staffing shortages, 2) Training frequency, and 3) Decentralization.

Staffing Shortages

A shortage of trained IT employees, and the strain of ever-increasing workloads affect quality of service and cyber-attack readiness. For example, implementation of body cameras for uniformed police officers requires additional training and maintenance for IT staff in addition to data storage. During interviews with various county departments, all interviewees noted being understaffed with open IT positions. In February 2021, Contra Costa County Health Services had 13 unfilled IT positions. As of November 2021, the County has several IT openings with a salary range between $74,000 to $140,000. The County is having difficulty hiring experienced staff to implement state-of-the-art IT tools because qualified cyber security personnel are in high demand nationwide. Based on Grand Jury interviews, the County cannot match private industry's compensation packages. While there may be better job security and long-term benefits working for a government agency, the competitive salaries and enticements like stock options, profit sharing and in-office perks pose competition to the County.

> IT executives see the talent shortage as the most significant adoption barrier to 64% of emerging technologies, compared with just 4% in 2020, according to a new survey from Gartner, Inc. A lack of talent availability was cited far more often than other barriers this year, such as implementation cost (29%) or security risk (7%).
>
> Talent availability is cited as a leading factor inhibiting adoption among all six technology domains included in the survey – compute(*r*) infrastructure and platform services, network, security, digital workplace, IT automation and storage and database. IT executives cited talent availability as the main adoption risk factor for most IT automation technologies (75%) and nearly half of digital workplace technologies (41%). (https://www.gartner.com/en/newsroom/press-releases/2021-09-13-gartner-survey-reveals-talent-shortages-as-biggest-barrier-to-emerging-technologies-adoption)

Even though there is limited IT talent available, the County could be more competitive with its compensation packages to attract more of these scarce resources. During interviews, it was evident that work-life balance is a significant issue for all IT

departments. IT staff shortages lead to increasing employee burnout and turnover. If the County were able to fill gaps in IT staff, the workload would be more manageable, creating a better work-life balance. Some private enterprises have developed skilled labor pools of IT specialists to cover temporary shortages in multiple departments. A pool concept reduces the need to increase staffing across many departments and is an efficient way to address chronic staff shortages. Also, a talent pool concept can be used as a training platform for new hires.

Training Frequency

The county currently has a three-part IT Security training program. The following is from DoIT's website:

1. "Information Security – This program covers prudent business practices that will establish and implement "the need to know" rule base. It dictates how county-controlled assets, both physical and logical "computer," are maintained with integrity, security, and monitoring.
2. Security Awareness - This grass roots program will ensure all County employees thoroughly understand and acknowledge that protection of County-controlled assets is critical to the survival and well-being of the County, as well as themselves.
3. Business Resumption (*BRP*) - This program ensures business continues after any significant business interruption. BRP is the overall umbrella that covers disaster recovery, emergency preparedness plans used by individual department and Individual employee's personal recovery capability."

Industry experts point out that unsuspecting employees often initiate cyber-attacks by opening emails with attachments containing malicious software or employees plugging in hardware such as flash drives or memory sticks to capture or corrupt network data. Based on Grand Jury interviews, industry experts recommend restricting the use of any personal devices at work and work devices at home especially flash or thumb drives. Based on our interviews, County employees and officials are still using personal devices connected to county computers.

DoIT is working to make this above training mandatory. With the increase in threats, DoIT will be requesting annual training. Currently, county-wide training is neither annual nor mandatory.

Decentralization

Based on interviews, the Grand Jury identified the decentralized structure of IT within the County as a potential source of vulnerability to cyber threats. Interviews revealed that there are at least three reasons for this vulnerability.

First, small departmental IT staffs do not have the time to perform necessary hardware and software updates on a regular basis. This undermines the security of data and systems in these departments and the entire County.

Second, the email systems used by County departments have their own domain names. “Because of spam, it is becoming increasingly difficult to reliably forward mail across different domains, and some recommend avoiding it if at all possible.” (John Levine (2008-10-15). "Users Don't Like Forwarded Spam." CircleID Retrieved 2008-11-07.)

Third, DoIT has procured state-of-the-art software programs to monitor network and email domains across the County. DoIT has also built cloud and server protections that are expandable for individual department needs. However, DoIT does not have the authority to mandate use of these capabilities county-wide. Based on our interviews, there are some departments that are either unwilling to utilize these products and services, or unable due to obsolete equipment or lack of available staff. Currently, the County does not have consistent methods or policies for ensuring that all County computer systems are protected from a cyber-attack.

FINDINGS

F1. County IT Departments are chronically understaffed.

F2. Obsolete equipment poses a vulnerability threat to County IT security.

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

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

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

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

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

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

F9. Decentralized IT structures increase vulnerability to cyber-attacks.

F10. The County's IT structure is decentralized.

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

RECOMMENDATIONS

The Grand Jury recommends that:

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

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

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.

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.

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

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.

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

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.

REQUIRED RESPONSES

	Findings	Recommendations
Contra Costa County Board of Supervisors	F1 to F11	R1 to R8.
Department of Information Technology is invited to respond	F1 to F11	R1 to R8.

These responses must be provided in the format and by the date set forth in the cover letter that accompanies this report. An electronic copy of these responses in the form of a Word document should be sent by e-mail to ctadmin@contracosta.courts.ca.gov and a hard (paper) copy should be sent to:

Civil Grand Jury – Foreperson
725 Court Street
P.O. Box 431
Martinez, CA 94553-0091