ALAMEDA-CONTRA COSTA TRANSIT DISTRICT

STAFF REPORT

MEETING DATE: 9/9/2020 **Staff Report No.** 20-202

TO: **AC Transit Board of Directors**

FROM: **Michael A. Hursh, General Manager**

SUBJECT: **Balancing Cybersecurity Controls with Productivity**

BRIEFING ITEM

RECOMMENDED ACTION(S):

Consider receiving a briefing on the District's approach to Cybersecurity control as it affects productivity. [Requested by Director Peeples - 10/9/2019]

STRATEGIC IMPORTANCE:

Goal - Financial Stability and Resiliency
Initiative - Infrastructure Modernization

This briefing item will allow the Board to take a fresh look at Information Technology Policies, get an update on newer risks associated with Cyber threats, and understand productivity impacts due to extra measures being put in place following recent Cyber events.

BUDGETARY/FISCAL IMPACT:

This is a briefing item and has no fiscal impact.

BACKGROUND/RATIONALE:

Due to exponential growth in deployment of Information Technology based solutions in Transit, everything is connected to the enterprise network, not to mention the tremendous growth in computers and smart devices in normal business operations. Most of the District's systems collect and generate a tremendous amount of data. Bus engines, traffic control systems, security video systems, ticket vending machines, operator badge systems, and even the facilities Heating Cooling & Ventilation Systems are communicating with other components, either generating data or consuming data. This connected enterprise makes the network vulnerable and subject to major cybersecurity risks. A single wrong click to a malicious websitecan provide access to hackers to disrupt the entire District operations.

Over the last several months, the District has increasingly become the target of malicious actors looking to exfiltrate personal information, accounting, and financial data. According to InfoTech, the transportation industry has been the favored target for cyber-attacks where state sponsored threat actors seek to disrupt operations. In another report by the FBI, Business Email Compromise attacks cost organizations an estimated $1.77 billion in losses in 2019, and the number of attacks has quadrupled since the start of the COVID-19

pandemic. As the District becomes more dependent on Information Technology, efforts to disrupt the District's operations, to steal, corrupt or destroy data, or divert funds, have increased. The perpetrators of the cyber-attacks have expanded, and their skills and sophistication have significantly increased.

Email/SPAM Filtering

Email is one of the most widely used business tools across the entire District. Second only to web traffic in volume, email is a primary mode of communication for the District to the outside world. Over 10,000 emails per day and over three million emails per year are generated and processed by the District. The District must secure this entry and exit point with consistent and complementary technologies.

AC Transit depends on an Email Security Gateway to filter all incoming email for spam, phishing and spear phishing attacks. Unfortunately, the current solution has a high rate of False Negatives (allowing bad emails) and False Positives (blocking valid emails).

Current process for Monitoring the Email Security Gateway for False Positives/False Negatives -

The Cybersecurity team monitors the email security solution daily for False Positives/False Negatives and takes appropriate action. However, it is not possible to manually monitor over 10,000 emails that the Districts processes daily. Once staff has an advanced email security solution in place, many of these mitigation action steps will be handled by the software engine.

The Cybersecurity Team is in the process of conducting Proof of Concept (POC) with leading Email Security Gateway solutions vendors, who offer an advanced threat monitoring and detection capability, leveraging Machine Learning and Artificial Intelligence technologies.

Web Filtering

The District does not have dedicated web filtering software technology in place today, but instead leverages its Firewalls to filter websites. The web filtering offered by the Firewalls simply categorizes websites. The technology uses several methods including rest analysis, exploitation of the web structure, and human raters. Users can notify the firewall vendor if they feel a web page is not categorized correctly, so that the service can update the category. It includes over 45 million individual ratings of websites that apply to more than two billion pages.

Current Setup to "White List" any websites for the District -

The White Listing of websites is a process to allow legitimate sites that may be otherwise blocked i.e. Malicious domains or Phishing sites. There is a small chance, less than one percent, that a legitimate website is blocked due to software flaw, however, a good site can be added fairly quickly by notifying the Help Desk.

A next generation web filtering software will allow AC Transit to have more granular control over allowed and non-allowed sites.

The Cybersecurity Team regularly monitors the Firewall logs and independent threat feeds and adds any new malicious URL's and IP addresses daily that have not been automatically updated on the Firewall database. In addition, the Innovation and Technology Department is looking into leveraging a free service offered by the Center for Internet Security to automatically filter malicious sites. This will prevent our systems from

connecting to harmful web domains, helping to limit infections related to known malware, ransomware, phishing, and other cyber threats.

While the District has made significant progress in building a Cybersecurity practice, the threat landscape is constantly evolving amid rapid technological change. To combat this risk and prevent operational disruption, a balanced approach towards security is required to provide suitable preventive and mitigation controls and to build a productive work environment.

ADVANTAGES/DISADVANTAGES:

There are no disadvantages to receiving this briefing.

ALTERNATIVES ANALYSIS:

There is no alternative to receiving this briefing.

PRIOR RELEVANT BOARD ACTION/POLICIES:

Board Policy 440 and Related Administrative Regulation

ATTACHMENTS:

1. Administrative Regulation No: 440B Information Security

Prepared by:
Tas Jalali, IT Manager - Cybersecurity

Approved/Reviewed by:
Ahsan Baig, Chief Information Officer
Jill A. Sprague, General Counse