Board Summary Report

Date: January 16, 2020

To: Board of County Commissioners

From: David Bessen, Director, Information Technology

Subject: Cybersecurity Update

This study session is to provide an update to the Board of County Commissioners on the state of IT's cybersecurity and IT's efforts to enhance our cybersecurity posture and capabilities.

Background

In April 2019, the County hired its first cybersecurity analyst, Amber Winthers. With the creation of this position, the IT Department integrated the various cybersecurity planning, testing, training and compliance efforts under a single individual for coordination and monitoring. IT also moved the locus of cybersecurity work out of the Infrastructure Division so that the Cybersecurity Analyst reports to the Department Director with the ability and backing to work effectively across all IT divisions.

Since filling the position, numerous activities have occurred, and plans have been established. IT assessed how well the County met the Center for Internet Security (CIS) controls. From the assessment, a project was designed for improving our cyber security readiness. The project contains several implementation groups, each with a set of tasks (controls) that will need to be completed. Most of the work involves documenting the controls that we already have in place.

IT also completed the annual Nationwide Cybersecurity Review, based on the NIST Cybersecurity Framework. Completing this review allows us to benchmark ourselves against other governmental agencies and establishes our eligibility for DHS grant funding.

A network security monitoring service—called Albert—was implemented in mid-2019 with the cost covered by DHS for the first two years. This system provides for centralized monitoring of network intrusions and provides alerts for traditional and advanced threats, which would help us identify and respond to malicious activities against our network.

IT also conducted a penetration test in October-November 2019. The test, conducted by a third-party, tested both our perimeter cyber defenses (our firewalls), as well as our internal firewalls that we installed a few years ago around our two data centers. The test results were very good with no significant vulnerabilities found on the perimeter. Some remediation was recommended for the internal firewalls and that has already taken place.

The Cyber Analyst has also begun formalizing and documenting cyber Incident Response plans, beginning with a 'playbook' for our service desk to use in the case of a cyber incident, such as a phishing attack.

A new cybersecurity testing and training platform was procured in October 2019 and a phishing test was conducted on January 9-10 to establish a baseline of susceptibility to phishing emails. The baseline level of "clicking through" was well below the 20% frequently seen in global reports; our click-through rate was just over 9%. The platform has

training courses available (through Arapahoe Learns) and IT can report on which employees have taken the training. Future tests can also be given to assess the training effectiveness and the improved "resistance" to phishing emails.

IT has also worked closely with the Office of Emergency Management to ensure that our plans were in concert with the cybersecurity hazard plans of the OEM.

Finally, the Cybersecurity Analyst has developed and delivered several training programs for departments or teams to help employees become more "cyber aware", to practice safe computing and to report anything unusual in the computer usage to the Service Desk, so that IT may responded appropriately to a real or perceived threat.

Links to Align Arapahoe

Discussion

Maintaining a secure computing environment impacts all three of our Align Arapahoe goals. A cyber breach could impact our ability to deliver services, could be costly (in resources and reputation) to remedy and could impact the quality of staff and citizens' lives. Maintaining and enhancing our cybersecurity posture reduces the risk of a cyber incident and, in the case of a breach, improves our ability to respond appropriately.

Alternatives

None.

Fiscal Impact

All the costs of the improvements implemented to date were included in the 2019 and on-going operating budget of the department, except for the DHS grant for the Albert monitoring.

Concurrence

Finance
Attorney's Office