Joint Administrative Services Board
July 22, 2019 Regular Meeting 10:00 am

At a regular meeting of the Joint Administrative Services Board held on Monday, July 22, 2019, at 10:00 am in the Meeting Room AB, Berryville Clarke County Government Center, 101 Chalmers Court, 2nd Floor, Berryville, Virginia.

Members Present: David Ash, Sharon Keeler, David Weiss

Members Absent: Chuck Bishop, Chip Schutte

Staff Present: Tom Judge, Brian Lichty, Gordon Russell, Ed Shewbridge, Brad Shumaker, Brianna Taylor

Others Present: None

1. Call to Order - Determination of Quorum

   At 9:57 am, Vice Chairman David Weiss called the meeting to order having determined that a quorum was present.

2. Approval of Minutes

   David Ash, seconded by Sharon Keeler, moved to approve the May 20, 2019 minutes as presented. The motion carried by the following voice vote:

David Ash	-	Aye
Chuck Bishop	-	Absent
Sharon Keeler	-	Aye
Chip Schutte	-	Absent
David Weiss	-	Aye

3. Health Insurance Advisor

   Tom Judge stated that $2,000 was budgeted for the Health Insurance Advisor and a procurement was completed. Chuck Bishop and Tom Judge ranked the three proposals in the following order McGriff, Gallagher, and Innovative. McGriff is an insurance company located in Winchester that was formally JV Arthur; the employee representative is Ed White who was our Anthem representative in the past. The representative has experience in giving health insurance advice in this geographical area. McGriff was contacted, the price was negotiated, and ultimately they stated that they would not charge. Meeting between McGriff representative Ed White, David Ash, Chuck Bishop, and Tom Judge is set up for August 6, to have the initial conversation on how things are currently set up and

what things could change to improve insurance options. Hope to have initial results for the Board by the end of August.

Vice Chair David Weiss asked what the better option was: to go with other insurance companies or to rearrange the current Local Choice methodology.

Tom Judge stated that he believed that Ed White would suggest that you would not know until you search for proposals. Tom Judge added that switching insurance is disruptive to employees and there is cost to searching other insurance companies. Unless Ed White suggests that switching insurance companies would be very beneficial then Tom Judge does not see that in the end we would risk disturbing everyone's current medical arrangements in order to leave Anthem.

4. Cybersecurity

Tom Judge Highlights:

- There have been regular episodes of security violations on systems across the country.
- End users are the ones that are attacked the most.
- Not all end users have the training to spot the attacks, which allows for easier access into the system.
- Attackers will alter an end user's computer and the end user will call IT to help. When IT is in the computer and using administrative passwords, the attacker is watching and gaining all of that information, which then can be used to hack the rest of the system.
- Need to find a way to get the employees to take the risk seriously.

Gordon Russell Highlights:

- Described the scenarios of the cases in Baltimore and Florida.
- Baltimore case all data was stolen but the locality decided not to pay the ransom, which will cost them more in the future.
- Florida case all data was stolen but the locality paid the ransom in order to try to get their data back.
- Florida case was a smaller locality (15,000 to 30,000) but the perpetrators walked away with half a million dollars.
- Expect that more small localities will be attacked.
- Combination of poor IT structure and end user email training.
- Email phishing is one of the main ways of attack; and once an end user clicks on a link, the perpetrators spend weeks in the network probing around for detailed information and steal the network data.
- Our IT strives to keep the system up to date and keep the network controlled and current, which is still not enough.
- No matter what IT does there is always the potential of risk.

- IT for both the County and the Schools feel confident in the backups and that if the system is compromised that a backup could be used to restore data.
- End users are the main target of attacks; and, if the end user is not trained, then the system network could be compromised.
- IT feels that it is important to educate all end users to the be skeptical of each and every email that comes into their inbox before they click on any links or open any attachments.
- Some ideas to improve awareness throughout the organization are reminder emails, phishing attacks, and training.
- There are companies, cost unclear, that complete these security awareness campaigns, they will attack the organization with phishing attempts and keep track of each employee over a few month period and then send a report to IT stating whether the employee passed or failed and then send helpful training tips for employees.
- There is a Google online training that is free that steps you through scenarios and tests you while you step through the process.
- This allows end users to look more in detail at the email. For example the name of who it is coming from, is the link actually the link that is written in the email, etc.
- Using same passwords at home and at work is a poor protocol to follow because then the perpetrators can get both into the work system and also attack any home devices.
- Logging out of the desktop computers at the end of each day means the computer is locked out of any user accounts and allows for any updates to be complete during the night, instead of shutting the computer down each night and having the updates occur once turned on in the morning.

Ed Shewbridge Highlights:

- School IT launched its own phishing attack about a year ago and approximately 33% of staff put in their email and password.
- Tested and trained staff to be more aware of the incoming email address and the message.
- During the phishing attack, IT discovered that one of the schools front desk personnel, who had seen the email earlier than most of the other staff, sent out an email to all staff warning them that the email that was just received did not look normal and that it should be deleted and to not click on anything within the email.
- In another school one of the teachers thought it looked different and also warned the staff.
- Found that within our buildings a few personnel are super aware of the attacks and try to warn all the other staff members.
- Constantly enforcing the safe computing practices:
    - Hardening passwords and not “remembering” them in memory.
    - Avoiding the re-use of the same password across multiple sites.
    - Logging out or sleeping computers when leaving the room.
    - Unsubscribing from SPAM emails.

  - Using encrypted websites when available.
  - Backing up data stored on individual PCs to non-networked media.
  - Restricting web surfing activity to legitimate work related sites.
- End user awareness and education is very important.
- Brad Shumaker put on a training presentation for some of the teachers to demonstrate what happens if a link is clicked on. Once they clicked on the link, Brad Shumaker showed them what he could do by having complete control over their computer.
- IT suggests that if something looks different, just delete the email. If it ends up being important, then the person will contact you in a different manner.
- Website restriction is used at the schools and there is always a struggle between restrictive and non-restrictive.
- Restrictions are different for the students and the staff. All go through the Children's Internet Protection Act (CIPA) filter but teachers have more access to websites.
- Both security awareness companies and employee educational programs are needed to better educate the end users but even then both may not be enough.
- School staff have been encouraged to use a password manager.
- Scans are being done to see what weak passwords are being used.

Next steps would be:

- Look at the cost of end user training vendors to get details, approach, and cost.
- Talk to insurance company to see mode of operation.
- Send out another reminder email to all employees with tips and tricks.

5. Next Meeting

August 26, 2019 (if needed)

6. Adjournment

At 10:49 am, Vice Chairman David Weiss adjourned the meeting.

_____

Minutes Recorded and Transcribed by Brianna R. Taylor