

City of Olmsted Falls
Minutes of a Council Work Session
Tuesday, February 25, 2020, at Olmsted Falls City Hall
26100 Bagley Road – Council Chambers, 6:30 p.m.

Council President Stibich called the meeting to order at 6:30 p.m. Roll call was conducted. Councilmen Lori Jones, Jennifer Jansen, Jay McFadden, Cornel Munteanu, and Brian Chitester were present. Yvonne Buchholz was excused. Others Present: James Graven, Mayor, Andrew Bemer, Law Director and Odis Rogers, Police Chief.

Bailey Communications Discussion

Mr. Bemer asked what Mr. Oswald would suggest that the City does to ensure the hacking does not happen again. Mr. Oswald stated that there is a new firewall that has security services running on it that does finger printing of traffic flows through the firewall, anything coming in or going out, which will stop viruses or anything that matches a signature. Mr. Stibich asked if this was put into place. Mr. Oswald replied no this was included on his proposal. Mr. Bemer asked if that was given to anyone. Mr. Oswald replied the finance department. Mr. Bemer indicated that the proposal should be distributed to Council as they will need to make the decision.

Mr. Chitester asked if Mr. Oswald proposed what he would recommend besides the sandboxing. Mr. Oswald replied a better email security. There is a program called fishline which basically performs spearfishing attacks on the organization. It will send fake emails to try and get people to click on things, if they do it is recorded and then the individual would go through training. This would be another way to test users and get them savvier with email. Mr. Stibich stated that this would catch people who are opening virus laden emails or files. Mr. Oswald stated that another recommendation is the sandboxing firewall, this program performs sandboxing and behavioral analysis. So, if something acts like a virus it gets blocked, if it is sandboxed or does something that is malicious it will block it. Mr. Bemer stated that he understands that Mr. Oswald has worked with the police department for quite a few years and asked if he has dealt with other police departments that are not necessarily tied into the city and have separate systems. Mr. Oswald replied yes, Bay Village, Westlake, Brooklyn, Olmsted Falls, Russel Township, Pepper Pike, Warrensville, University Heights, and Avon Lake. Half of what he does is law enforcement, local government and large school districts. Mr. Bemer asked if the city wanted an IT person on staff what would be the associated costs. Mr. Oswald asked if that would be for full time. Mr. Bemer replied yes. Mr. Oswald indicated that it would probably be close to \$100,000.

Ms. Jones stated that she is surprised that no one has asked for a Sock 2. Mr. Oswald replied that these reports are geared towards financial institutions like banks. Ms. Jones stated that it's not just for them it can be for anybody. Mr. Oswald replied it is geared towards that. Ms. Jones replied that it depends on how Bailey is protecting the city's data. Mr. Oswald replied that this is why the city goes through the LEADS audits as they want to make sure we are doing things properly here because it is people's records, social security numbers, addresses, photos, etc. Ms. Jones replied right, but who evaluates the LEADS system to make sure that everybody is doing the right thing. Mr. Oswald replied LEADS. Ms. Jansen replied the state. Mr. Oswald stated that they send someone out and go through the city's system, firewall, switches, servers, and everything. Ms. Jansen asked if that audit

was every two years. Chief Rogers replied that it is every two years. The department was just audited by OHLEG, which is the attorney general's office. One of the things he had to provide was documentation that the employees of Bailey Communications have been finger printed, the background checks of those finger prints, and the paperwork that shows that they are compliant with everything. This happens every two years. He would like to comment regarding the police perspective. He indicated that Mr. Bemer asked how to keep this from happening again, the answer is you don't necessarily keep it from happening again. Everyday there are new things coming out which is how the city got hit with this, and Bailey's job is to make sure that this particular virus does not happen again, but we don't know about the next one. The important issue for him and the data that is downstairs, years and years of records, things that we have to keep Bailey has stored off site. Within three days we have all of our information back and are up and running again, had we not had that, it would have been catastrophic.

Ms. Jones stated that if Bailey did an evaluation for Olmsted Falls you would say that what is on the police computer, the LEADS, is important so that would be the first priority, to get them up and running. She asked if the firm that performed a forensic analysis provided a report. Mr. Oswald replied yes. Ms. Jones asked if Council could have a copy of that report. Mr. Oswald replied yes. He indicated that the biggest challenge in getting the system back online was that the computer forensic company required us to make copies before we could restore the system because they needed to see hard drives in the state they were in before we could overwrite and restore the system. We had to provide copies of the server hard drives, copies of ten or eleven computers, and after all that work, we were then permitted to restore the system. When we began restoring, we had to be very careful because the ransomware was also attached itself to the back up's. The things that were set up to do the ransomware attack and encrypt things were also in the backups. We restored the system prior to the encryption and then had to work backwards to determine where the virus was, how it was working, what it was talking to, and stop it so when zero hour hit again it did not encrypt everything again. It was very complicated.

Ms. Jones asked Chief Rogers when the system had the ransomware was he able to use another city to obtain whatever information he needed. Chief Rogers replied that everything was handwritten until the system came back up. Ms. Jones asked if there was information needed that made it more complicated. Chief Rogers replied that his department could still run LEADS and get information, for example, he believes Ms. Jones is referring to officer safety issues. If an officer made a traffic stop and since our computers were down, how would the officer know if the person being stopped had a felony warrant, Strongsville's computers were still up and running. Ms. Jones replied he could use them. Chief Rogers replied yes, we use them every day for that purpose and they relay the information to us via radio. He is talking about the in-house computers that we did not have access to. The CAD log, which is information that happens every day we did not have to handwrite because dispatch enters the information into their CAD system and once we are up and running it is paired back up. So, if he had to create a document for Council, for example, he would not be able to do that he would have to hand write it or go to a typewriter or use his home computer and once we are back up and running he would transfer the file. Ms. Jones replied that was okay as long as he could still obtain the information he needed. Chief Rogers replied that this is quite frankly one of the benefits of having off site dispatch.

Mayor Graven stated that Mr. Oswald indicated that is was a high probability that it came from Russia or knew for sure. Mr. Oswald replied it was Russia, it is a group called Ryuk. Mr. Stibich stated that he would ask that the report that Ms. Jones requested be sent to the Clerk so that it can be

forwarded to Council. Mr. Oswald replied that he would and believes that the report was sent to Ms. Veloski as she was the one working with the insurance company and contact for Crypsis so he believes that she has that report. Mayor Graven stated that he believes the insurance company did cover the costs of Crypsis. Mr. Bemer asked if Bailey was also paid. Mr. Oswald replied yes. Mayor Graven replied that Bailey was also paid by the insurance. Ms. Jones asked if the city had to pay a large deductible. Mr. Oswald replied no, the deductible was \$2,500. Mr. Bemer asked if what the costs were to the insurance company. Mr. Oswald replied \$90,000. Ms. Jones asked if that was for the cyber security firm. Mr. Oswald replied that he believes their bill was close to \$70,000.

Mr. Munteanu asked if EMS or fire reports were affected. Mr. Oswald replied that the information stored on the Cloud was not affected, but the information that was local had to be restored. Ms. Jones stated that fire also used Strongsville Dispatch so they were okay for EMS. Mr. Munteanu replied that the reports are all located online. Mr. Oswald replied that the fire department was able to access that information. Mr. Munteanu replied that the department has the external server in the watch office.

Mr. Oswald replied that as a result of this issue Bailey has cut off outside communication with other countries besides the United States so there are more restrictions, unless an exception is made by Bailey. The email system has also been updated so if a server is outside of the United States it will be blocked. Ms. Jones stated that she asked that question if any of the servers where the data was bouncing around was outside of the United States cause every country has different requirements. Mr. Oswald stated that there is a lot more restrictive unless there is some sort of exception that needs to be made.

Mr. Chitester stated that the cost of Bailey's recommendations is \$9,324.30. Ms. Jones asked if a vulnerability test was performed to determine that this is what is needed. Mr. Oswald replied that these recommendations are components that the city should have. Mr. Chitester stated that if the city only had the funds for one of the recommendations, what would that be. Mr. Oswald replied the Sonicwall Capture Client which is the sandboxing. Anything that gets through the firewall because it is unknown or matched a rule and was allowed in, or comes through email, if it gets through all of that it is on your computer and all someone has to do is click on it so that capture client actually looks at the attachments and opens it up and sees if its malicious and if it is then it is blocked and will perform behavioral analysis. This is the most comprehensive system. Mr. Chitester asked if this would be something the administration would like to see happen in the next 45 days. Mayor Graven replied yes. Mr. Chitester indicated that he does not want to see the city go into the red because we need \$10,000 because if we can just get one now and save some money, unless we can handle all of the recommendations. If we can only purchase one now, we can then consider additional purchases for the next few years.

Ms. Jones stated that we have a system and Bailey oversees it and updates the firewalls and monitoring, so what kind of protection do you give as our base. Mr. Oswald replied that the city has Trend Micro as antivirus and is worry free business security, the city also has a Sonicwall firewall, the current email security is Barracuda security gateway, there is also a Cloud protection layer, which handles geo fencing. He stated that there is also Barracuda backups so if something happens Bailey can recover data manually or the system as a whole.

Mr. Chitester asked if we are able to isolate police, fire and EMS on a separate side and have a division between city administration and Council stuff, so if one gets infected it does not spread to

everyone. Mr. Oswald indicated that you could but the issue is that it is active directory, even if the computer is on a different networks the way the virus spreads is by talking to the server and obtains every computers name by performing DNS requests to obtain the IP address and then tries to connect to the computer. So, no matter what Vline it is on or where it is in the network it will get hit. Mr. Chitester stated that even if we isolate and split them off, they can still be hit. Mr. Oswald replied that the only real way to complete this is to have a firewall in between the two segments. Mr. Chitester stated that he would rather see the city have to deal with an attack and have the police and fire kind of protected then vice versa. Ms. Jones asked if Bailey has a diagram of where the firewalls are. Mr. Oswald replied yes and is the same information that is given to LEADS every year. Ms. Jones asked if that was for the whole city. Mr. Oswald replied yes. Ms. Jones asked if he had a copy. Mr. Oswald replied not on hand but could send her a copy. Ms. Jones stated that she was an IT auditor and did not just do financial institutions when she did the EDP audit, we just did for evaluation and were told that no one should ever hire anyone that doesn't get a SOCK. Mr. Oswald replied that the audits that the city goes through years are more comprehensive than a SOCK. They ask about all the controls and on the police side there are a lot of different requirements and then fire has audits as well, there are a lot of hoops that Bailey must go through every year to make sure we are compliant. Some of our cities have credit card processes and then we have to complete PCI compliance, LEADS compliance, and then the state auditor's audit and then the financial firms that cities have come in an audit.

Mr. Bemer stated after reviewing the proposal with the hardware identified and the licensing that has to be renewed every year the city is looking at \$7,000 with a one-time installation of \$2,400. He asked how often we would have to go through new hardware. Mr. Oswald replied that included in the proposal is a Sonicwall firewall which comes with a three-year subscription so the city would not pay anything for three years, because it is a bundled package. Mr. Bemer stated that the other part is the hardware and asked if we would be replacing anything that would reduce our costs. Mr. Oswald stated that the Sonicwall capture client is a yearly subscription, the Sonicwall secure upgrade will replace the current firewall and is actual security compliance and firewall, this comes with a three year subscription and then would cost approximately \$900 each year for renewal, the fishline is the simulated spearfishing attacks that tests users to determine where there are holes. Mr. Stibich asked who would monitor the fishline. Mr. Oswald replied Bailey. Mr. Stibich asked what would happen if someone were to open an email. Mr. Oswald replied that the system runs itself. Bailey would be alerted and in turn would talk to that employee and let the department head know. The employee would then go through training and be tested. There is an entire portal that shows who clicked on what email and what was contained in that email. Ms. Jansen asked if there was any training that could be provided to Council prior to catching someone. Mr. Oswald replied yes. Ms. Jansen stated that after the three-year subscription the costs to the city each year would be \$6,000. Ms. Jones replied that the costs after the three years would be \$900. Mr. Oswald replied that the yearly costs for all the recommendations would be roughly \$5,500 per year. Ms. Jansen asked what the city's current costs are for its current software. Mr. Oswald replied that the antivirus is approximately \$1,600 per year.

Ms. Jones asked if Bailey performed a risk assessment of the city or any kind of assessment to determine what was needed and why. Mr. Oswald replied no, these recommendations are things the city should have if you want to be the most protected. If you follow Guardner, they look at all the different technologies and compare them and these are the ones listed as technologies that people should have if they want to protect themselves. Mr. Stibich asked who Guardner was. Mr. Oswald replied that they evaluate technology protects and rate them. Based on those reports Bailey makes

recommendations. Ms. Jones asked if Bailey did anything based on risk. Mr. Oswald replied no. Ms. Jones stated that some things may not need the top of the line equipment but some things might. Mayor Graven stated that if the city wanted to be perfectly safe, we would have to spend \$300,000 a year to be 99% safe. Mr. Oswald replied that there is no silver bullet for being safe. Mayor Graven replied that there is no way to be 100% safe even if we spent \$2 million a year. Mr. Oswald replied that if someone is trying to get in or trying to attack your organization you try to make an obstacle field for them to get through and then if all else fails you have a good back up that can be recovered which is what the city had. But there are other things that can make an obstacle course. Mr. Chitester stated that his previous question regarding the three recommendations how many cities, organizations or school districts that Bailey services have them. Mr. Oswald stated that fish lining is very new and believes there are two or three cities that have it, as far as line item #2 every client has it except for a couple with different firewalls. Mr. Bemmer stated that he is curious if Mr. Oswald has made any of these suggestions to anyone in the city previously. Mr. Oswald replied not all the items. Fishline is new, this sonicwall is recent because the existing firewall is going end support soon. Ms. Jones asked when. Mr. Oswald replied that he does not know off hand. Ms. Jones asked him to find out. She asked if he could give us, or is it in our agreement, what they provide and what the dates things will end. Mr. Oswald replied that the agreement is professional services, for us to maintain service, the antivirus is separate it's a yearly subscription and we track all of the renewals through our system and send estimates when they come due. Ms. Jones asked how far in advance the city is notified. Mr. Oswald replied 45 days. Ms. Jones asked if Council could get a list of when our renewals are due. Mr. Oswald replied yes, we prepare a budget for the city every year what is expected to renew. Ms. Jones stated that the \$17,000 was just renewed and is for one year which is just for services. Mr. Oswald replied yes. The agreement covers Bailey to be onsite once a week for three hours. We also monitor the network and are on call 24/7, so if the police department has an issue at 2 in the morning, we take care of it. Mayor Graven replied that the Police Chief did inform him that they have called them out at 2 am and on weekends and they are here. Mr. Oswald replied that he has even had some police cars roll through his driveway to get their MDT's fixed. Mr. Stibich stated that the alternative is to hire our own employee as IT. Mr. Oswald replied yes but for a small city that does not make sense.

Ms. Jones again stated that the \$17,000 was for services and all of the virus software that has to be renewed, what is the cost of IT to the city each year. Mr. Oswald indicated that he did not have that figure. Ms. Jones asked if he could obtain that information. Mr. Oswald replied yes. Ms. Jones stated that she would recommend that we have some sort of risk assessment or vulnerability assessment. Historically, she has seen companies, that provide services, give a risk assessment which does not usually cost extra as it is part of their service. Mr. Oswald replied that would have to be added to the contract. Ms. Jones replied that Bailey does not provide a risk assessment as part of the contract. Mayor Graven asked what the cost would be. Mr. Oswald replied that it would depend because that would be conducted by a third party.

Adjournment

Mr. Chitester moved to **adjourn**; Mr. Munteanu **seconded**. Voice Vote: 6 ayes; 0 nays. **Motion carried**. The meeting adjourned at 7:23 p.m.

Paul Stibich, Council President

Angela Mancini, Clerk of Council