DEPT./BOARD: **Information Systems and Security Advisory Committee**
DATE: 4/**11/2022**
TIME: **7:00 PM**
PLACE: **Virtual via Webex**

Meeting Minutes

Present: Chair Steve Morin, Vice Chair David Hughes, Glen Mills, Ben Axelrod, David Miller, Jose DeSousa, Joseph Bongiorno, Phil Pascale
Absent: Bob Cuhna

Posted Agenda:

1. Public Participation
2. Approval of Minutes
3. Cybersecurity Policy Implementation Progress / Other IT Projects Progress
4. Presentation to the School Committee on 4/12 for adoption of the Cybersecurity Program
5. Presentation to the Select Board on 4/25 on progress on the town side
6. Discussion on the proper disposal of existing MIS equipment
7. Adjournment

Public Participation

None

Approval of Minutes

Comments were solicited, and the minutes for March 14th, 2022 were seconded and unanimously approved.

Cybersecurity Policy Implementation Progress / Other IT Projects Progress

While the firewall was completed for the first policy implementation milestone, other projects have a while to go until completion. (For example, adapters are sought to bring 40/10 speeds.)

For compatibility with non-CASB technology, it's almost a 365-day wait: we are in contact with a vendor representative to bring the data center to new switches and into the core of the network. Once one item becomes available, all other items become available en masse but the wait is long. Bringing the data center into the core is in progress for fiber connectivity.

Added functionality on email security or CASB has not begun, but it may be easier to go through the school side first and the town later. Other vendor(s) may be available for more features on cloud security.

The meeting with Ways and Means last week got approval to hire someone to work a 19-hour/week tech job, but the hire still needs to be approved in town meeting next month. Nevertheless the outcome from last meeting is good and we're moving in the right direction.

As for the school side, we need to start prepping for the next financial year. Over 3000 iPads need to be purchased for students, but we may have the same problem: while we might put in an order for 5/10, to requisition by 7/18, but this may get pushed out later and later, for delays on arrival. We're working the kinks out with people on the school side. Normally we would talk to people in June, but not right now. (For example, last year the project was to replace projectors, but the order placed in 7/2 or 7/3 meant that the projectors were received 6 months later in Dec/Jan timeframe.) Access point times can be in excess of a year; AV equipment is 6 months to a year.

For configuring those devices, you have basically a couple weeks of work for thousands of devices. Student Information System (SIS) is where all student data resides, but Apple Manager and Google Classroom interface with it and the iPad can't be configured until those things are in place. All devices, even phones, can be removed and configurations lost accidentally, which means phones also need to be configured once more, especially for 911 calls. All of this requires a lot of advance planning.

Progress on cybersecurity policy is ongoing: there's going to be some outreach to department heads sometime in early summer. There are vacations happening, but there may be a lot of time to have conversations about implementation. Once all articles are completed, the timeframe becomes a lot easier apart from Ways and Means. The current plan is late May/early June to meet with department heads, unless IT has the bandwidth to do so sooner.

The hire approval doesn't become effective until the new financial year starts, plus there's onboarding time, so effective time for the new hire is probably early August: this means the cybersecurity urgency is there but there is no bandwidth to supply time. To alleviate some of this urgency and make implementation easier (without having to sit down with ISSAC), the plan is to get one large department involved and set up a template for other departments to follow.

The additional grant has been partitioned into two assignments:

1. Education on phishing attacks, multifactor authentication, PINs – this shows the same security problems from a variety of different angles, which is nice. This is refreshed every year to cover onboarding, absences, cycling employee/user issues.
2. A bit more standard rote education on concepts of cybersecurity and social hacking/exploits. This is more text-based: different scenarios ask users to come up with the correct answer in 5 questions, which are repeated with the wrong answer.

The difference this year is incorporating more video scenarios: leaving laptops open in a cafe, taking devices home to check email, leaving devices unattended – more illustrative content than previous years. The videos can't be bypassed, so time must be found so employees can be made aware of the scope of cybersecurity vulnerabilities.

The training isn't mandatory, but people do need it - to achieve maximum possible participation rate, we might use the example of state law-required conflict of interest training. On the town side, participation rate isn't 100% but we've had very good turnout.

Presentation to the School Committee on 4/12 for Adoption of Cybersecurity Program

This will look somewhat like the presentation made to the Select Board, which will emphasize more about the benefit to schools and less on the specifics of policy. The presentation includes the following requests:

1. Adopt the town policy
2. Appoint someone to take the lead in cyber activities
3. Immediately start work on essential preparedness plans
4. Train staff in specific responsibilities
5. Require 100% participation in annual phishing training
6. Simulated attack

As part of presentation, it's recommended that we emphasize the the costs and delays inherent in an attack on a school. The consequences would include compromised daily attendance systems, email, and school networks. One school district had to send everyone home with no means of working remotely. A ransomware attack threat means that processes have to be in place if the ransom is paid, or processes for data loss and recovery if the ransom is not paid. Plans are important to develop in advance, rather than trying to put together in the midst of an incident.

There is no town or school that does not require email today, and yet email is the number one attack vector for malware: studies have shown this fact, year after year.

Therefore, the thrust of the presentation is that municipalities and school systems in particular are prime targets for malware, and no school should be the next victim. The costs to schools are many:

1. Direct financial cost of ransomware attack
2. Inability to take attendance
3. Inability to timely fulfill state reporting requirements
4. No network for lesson plans
5. Records affected: health, disciplinary
6. Ransomware leverage is a public school safety issue
7. Reputational damage, individually and institutionally

Even an occasional user of the system could be indirectly responsible for bringing down the entire system without training.

Presentation to the Select Board on 4/25 – Progress on the Town Side

Update: good first summer and early fall last year with education on the importance of cybersecurity. The next step is to be able to build out charts that have complete cyberpreparedness participation, and therefore get meetings with the department heads and a preparedness plan.

Over the past couple of months, things have slowed down a bit with other priorities, but the goal is still to get one department to build out a cyberpreparedness template: where the data reside, progress on training compliance. To ensure better compliance over time, it's recommended to ensure participation as part of job criteria.

ISSAC is looking at training duplication between town departments as an opportunity to streamline and have central funding. If the town police have MIS people, it's possible to leverage more efficiencies by having a larger MIS department and have people working across the entire town and sharing information, rather than in silos.

One area of concern is related to more critical systems, i.e. 911 or sensitive information including ongoing investigations or crime reports that aren't necessarily public.

It may help to get statuses from various departments over adoption of cybersecurity policy, and any issues identified.

Discussion on the Proper Disposal of Existing MIS Equipment

Breaches can happen from dumpster dives for old laptops, and old account information retrieved. Properly disposing of old data and equipment will include proper data and document shredding techniques.

We already have a good process in town, where one person on the team collects hard drives out of every machine and passes the drives to an archivist who keeps them in a storage safe for 2 to 3 years. After that, the drives are brought to shredding, where the archivist watches them get shredded and receives a certificate of destruction.

For SSD drives, we're not recycling those yet, but erasing them according to DoD guidelines.

We write down every serial number, with separate rules for reusing equipment within the 2-3 year window. However, if the equipment is “zero value” or outside the window, it's shredded.

None of this is a new practice and has been done for many years now.

Adjournment