Technology Committee Meeting Minutes – October 11, 2011

-Approved November 8,2011 -

Attending: Chairman John Sauter, Vice Chair Tony Richardson, members John Lastowka showed up at 7:05, Curt Conrad, Brian McCarthy, Jamie MacFarland was excused. Also present Town Technology Coordinator Chuck Miller, Police Chief Mark Doyle and Assistant Fire Chief Anthony Stowers

Call to order by John Sauter at 7pm

Approval of Minutes:

Motion made by Tony Richardson, seconded by Brian McCarthy to approve the minutes of August 9, 2011 with a change that Tony Richardson seconded the minutes of July 12,2011.

Motion Passed 4-0-0

New Business:

1. A presentation was given of both Crimetrack and Firetrack software from Microsystems Products.

Motion made by Curt, seconded by Brian to recommend the Town go with the first option ($27,504) but also have a much more detailed scope of work, motion seconded by Brian
Motion Passed 5-0-0

Comments from the Press and Public

None

Adjourn

Motion to adjourn was made at 9:00 PM by John Lastowka, seconded by Curt.
Motion passed 5-0-0

Attached:

Technology Issues, October 11, 2011

1. Issue: Chuck Miller, though he has much experience, is not able to handle some problems.
    1. Analysis: Chuck lacks training in Microsoft Windows Server and Microsoft Exchange.
    2. Recommendation: Offer Chuck training in Microsoft Windows Server Administration and Microsoft Exchange Administration. Chuck stated that the budget for training has been about 150.00 but has paid for some training himself if he felt it was important enough. John L. asked if Chuck could get the cost of some of this training so the committee has an idea what a valid budget number should be.
2. Issue: Too much of the day-to-day operation depends on Chuck.
    1. Analysis: Chuck has taken too much responsibility onto himself.
    2. Recommendations:
        1. Document the IT infrastructure so someone else can administer it in case Chuck is “hit by a bus”. This will require an inventory of all IT equipment. Keeping the inventory document up to date will require that each piece of IT equipment have a unique, visible, inventory number.
        2. Document Chuck's procedures by following him around and writing down what he does.
3. Issue: The backup procedures risk non-public data being revealed.
    1. Analysis: taking unencrypted disks home risks losing them.
    2. Recommendations:
        1. Encrypt all backup disks, using Microsoft Windows full-disk encryption.
        2. Encrypt all backup tapes, using a technique not yet identified.

3. Store backup disks and tapes in a town-owned facility, under lock and key. Encryption is still needed because disks and tapes can me mislaid during transit.

4. When choosing a site for backup, it must be separate from the site where the data is normally used, to protect the data from a single-site disaster.

5. Eventually, each site which houses Town data disks or tapes, whether for regular use, for backup, or both, must have a signin/signout log to record the departure and arrival of disks and tapes. To make this work, each disk and tape must have a unique, visible, identifier.

4. Issue: Town Hall has poor physical security.

    1. Analysis: Too many people have door keys.

    2. Recommendation: Replace door locks with RFID key cards. Each person has his own unique key card, which can be invalidated without having to get it back from him. Different people can have the authority to open different doors at different times Curt will look into some costs for this type of system.

5. Issue: The Town is at risk of a lawsuit for software license compliance.

    1. Analysis: If Steve Balmer were to walk in tomorrow and demand that we prove license compliance, we could not.

    2. Recommendations:

        1. Find and put in a secure place all of the paperwork related to software licenses.

        2. Inventory all software used by the Town that requires a software license.

        3. For each piece of software for which we cannot prove that we have the necessary license, either

            1. purchase a license, or

2. stop using the software, or
3. replace the software by an equivalent software product that does not require a license, or
4. replace the software by a different licensed software product, and purchase the necessary license.

6. Issue: The Town's network is at risk from intruders over the Internet.
    1. Analysis: Not all the points of contact between the Town's network and the Internet are adequately protected. This includes the Police cruisers' access to Police through Comcast.
    2. Recommendations:
        1. At each point where any Town equipment interfaces to the Internet, provide a firewall which forbids any unauthorized messages.
        2. Where the Town is using the Internet to connect between Town facilities, make all traffic which pass between the Town facilities use a VPN.
7. Issue: There is no disaster recovery plan for the Town's IT infrastructure.
    1. Analysis: In the absence of a formal plan, much effort will be wasted trying to recover from a disaster, and the recovery will likely be incomplete.
    2. Recommendation: create a disaster recovery plan, which describes what to do if a single building is completely destroyed, with all its contents, and what to do if Chuck is “hit by a bus”. The exercise of writing the plan may suggest some changes in the backup procedures.
8. Issue: There is no plan for the future of the Town's IT infrastructure.
    1. Analysis: The Town's IT infrastructure has developed based on immediate needs—when something breaks we start thinking about how to replace it.

2. Recommendation: Develop short- medium- and long-term plans for the Town's IT infrastructure. This includes replacing workstations and servers as they reach end of life. Consideration should also be given to upgrading and replacing software.

9. Issue: Non-public data on workstations can be extracted and revealed using USB data sticks.

    1. Analysis: Network-based data protection does not consider moving data using “sneakernet”. Full-disk and folder-based encryption does not guard against copying data to a USB stick from a logged-in workstation.

    2. Recommendation: Create a policy concerning use of portable data storage. The policy needs to be enforceable.