PRUDENTIAL COMMITTEE FIRE DISTRICT #1
144 Newton Street
South Hadley, MA 01075

Prudential Committee EMERGENCY Meeting Notes

Meeting Date: September 21, 2018

Location: Fire District Headquarters, 144 Newton Street

This session is being recorded

Call to Order: 1:00 p.m.

Prudential Committee Members Present:		Michael Wozniak, Chairman (MIW) (via telephone)	
		Kevin Taugher, Clerk (acting chairman)	
		Bruce Perron, Member	
Other attendees:	Monica Walton (MW),	Kurt Schenker	Chief Authier
	Atty. Mark Beauregard	Corey Briere, (Complete IT Solutions, District Contractor)	
	William Schenker (WS)	John Mikuszewski	Jennifer Fernandes

- Call to order
  - MIW was out of the district and is participating via telephone conference call.
- Discussion and vote on Fire District Accounting Software that has been encrypted and being held for ransom
  - KT chaired the meeting in the place of MIW to facilitate the discussion.
  - The Fire District accounting software ("SoftRight") was hacked by unknown attackers and has been encrypted to prevent access by Fire District personnel.
  - MW reported that she attempted to use the accounting software late in the afternoon of Tuesday, September 19th. She was not able to gain access through any of the computers in the office.
  - The problem was reported the same afternoon to the District IT consultant, "Complete IT Solutions, Inc.". A representative was dispatched on Wednesday morning. The representative discovered that the accounting files had been encrypted, and the files could not be unencrypted by the IT consultant. It was then evident the files had been hacked and maliciously encrypted.
  - Later Wednesday, the IT consultants were in contact with the hacker and confirmed the files were being held for ransom.
  - MW reported that the two sets of backup files she had were also corrupted, as the backups were initialized on Tuesday morning, not knowing that the primary files had already been encrypted.

- CB explained that the District was subjected to a 'brute force attack' on the "RDP" (remote desktop). Somebody tried various names, got ahold of one of the names and used an automated program to attempt to use an estimated 40,000 passwords before breaking into the District software. CB believes it was a random attack.
- MIW asked for the details on what protections the District system must prevent such an attack. CB responded that previous IT administrators had disabled the secure password aspect of it, which enabled the use of weaker password protection schemes.
- CB said that there was no offsite storage of the primary files, but the secondary storage used by MW was corrupted during the Tuesday morning backup.
- BP asked what the recourse is to resolve this problem.
- CB stated that the only way to decrypt the files would be by obtaining the decryption key from the attacker.
- CB has received a few emails from the attacker. We acknowledged receipt of the ransom notice from the attacker, who demanded the equivalent of the amount of "one bitcoin" which has a current value of around $6,500. CB requested proof that the attacker (and ransom demander) could decrypt one of the affected files. The attacker did not respond to this request.
- Based upon the lack of response from the attacker, CB said that he does not recommend paying the ransom.
- BP asked about the potential for hidden programs that would enable the attacker to gain access again. CB said that the correspondence was through a separate gmail account, and steps would be taken to avoid future malicious access to the District server. CB recommends installing new hard drives to replace the existing drives that had been compromised, and fresh installs of all SoftRight software on the new drives.
- CB said there is no guarantee that paying the ransom would allow the District access to the encrypted files.
- The cost of new hard drives is nominal, only a couple hundred dollars.
- MW has been in contact with SoftRight and had received an estimate of $7,500 to $9,000 to reinstall and configure the SoftRight program on new server drives.
- CB says that the chart of accounts from an old server (through June 30, 2016) could be used as a starting point for reconfiguring the program, likely saving configuration time for SoftRight.
- It was identified that the root cause of the successful attack on the District server and software was insufficient password protection for remote access. Going forward, a much more robust access control system would be implemented. Gaining access via remote desktop will be configured through implementation of a VPN (Virtual Private Network) and then remote desktop access.
- MIW asked if the encrypted files included personal employee information such as Social Security numbers. MW said that was not the case. The normal payroll information is not included in the files that were encrypted. There are a few S.S. numbers for

individuals not paid as employees, but were issued on form 1099's, and for individuals earning less than $600.

- MW said that the process to assess the risk of sensitive data being compromised is an outside consultant's assessment of whether a "breach" has occurred, and if so, determine the extent of the breach and identify the reporting required by law. For those individuals affected by a breach, the District will have to pay for surveillance of those affected for some amount of time.
- MW distributed the terms of the District's insurance coverage for this event. There are three separate categories, computer attack coverage, cyber extortion coverage, and data compromise coverage, each with a $10,000 deductible.
- MB questioned CB on the issue of turning off password protection coverage by the previous IT company. CB couldn't comment on previous setups. CB stated his company would not set up password protection in that manner.
- KT said that the backup process used by the District should be reviewed to ensure it measures up to the current processes.
- CB said that going forward, a backup process would be established to backup to the Cloud with 30 days of storage which could not be accessed by anyone other than the Cloud service provider.
- MIW asked exactly what had been corrupted. MW responded that all active SoftRight files and data had been encrypted. Files through June 30, 2016 were available on an archived hard drive, and paper copies of details from July 1, 2016 through the present time were available. Payroll is all available, as those details are processed separately from the SoftRight program, and only the summaries are reported in SoftRight.
- An action item was named to find out from SoftRight exactly how much the legacy data would aid in the recovery process
- Interim actions are to process ongoing transactions until the software is back in service. MW mentioned handwritten checks for payroll and invoices, and warrants issued in Excel spreadsheets.
- MW said that the banks have been notified of this issue and all passwords and access has been altered to avoid the illegal use of the encrypted data.
- MW said that a forensic review of this incident had to be undertaken to determine if a "breach" (legal term) had occurred, and if so, that appropriate notifications would be made to anyone affected by the breach. No employee receiving a W-2 form had personal information in the encrypted data.
- Discussion on whether to pay the ransom and purchase bitcoin.
- BP asked what the IT costs associated with the recovery effort would be. CB said it would only be a few hours of his time, plus the cost of hard drives. Our system allows for one remote access at a time, and that could be installed on the two PC's that would use remote access in a secure manner. CB explained the access to the server.

- General discussion whether to pay the ransom. Since there is no assurance we will recover the data after paying the ransom, it doesn't make sense to pay it. Also, there was a consensus that paying ransoms is a bad precedent, which could lead to future attempts to extort the District.
- MW said that the SH police were notified, and the MA state police cyber security center and the DA's office were subsequently notified as well. Since this attack was over the internet, there is no way to trace back to the instigator.
- WS wanted to see if additional investigation could be followed up on. CB will be able to give law enforcement any backup information they may require.
- MIW asked how the District would go about paying for the recovery effort. There is a $20,000 reserve fund, and there is $10,000 in funds in the existing IT account.
- MW said that Tom Scanlon, District financial auditor, recommended that the decision on paying a ransom should be based upon the assessment of the District's IT consultant. Since our IT consultant has expressed concerns about trusting the attacker, that weighs against considering the ransom.
- KT said MW must follow up on ensuring we make all reports according to the law.
- MW said that after speaking with the insurance company, the forensics analysis will determine whether the District's data was 'breached.' If the analysis indicates a breach, then legal notifications will be required. If no breach, notifications will not be necessary.
- KT moved that the District Clerk-Treasurer pursue the resolution of this issue with the insurance company and the District's IT provider, and report back to the PC at the September 27th meeting with a status report and a rough estimate of costs. BP seconded. Motion approved, 3-0.
- KT asked to ensure that the corrective action from the IT perspective be explained at the next meeting. CB will be at the September 27th meeting for a follow-up

- Motion to adjourn
  - Meeting adjourned at 1:44 pm.

Voted and approved by the Prudential Committee on October 25, 2018.

A true copy, attest:

Kevin E. Taugher, Clerk