TOWN OF SUDBURY
Office of the Town Technology Department

278 Old Sudbury Road
Sudbury, Massachusetts 01776
Tel: (978) 639-3306
Email: thompsonm@sudbury.ma.us
Fax: 978-443-1033

Mark Thompson
Technology Administrator

Date:	November 27, 2017

To:	Division of Local Services

From:	Mark Thompson, Technology Administrator

Subject:	Community Compact Grant – Cyber Security Assessment / Upgrade summary

The Town of Sudbury hired Compass IT Compliance to conduct an External Vulnerability Assessment of our thirteen public facing IPs. The White box network vulnerability assessment was conducted on the Town's 13 external IPs utilizing the QualysGuard remote external scanning system. The White box vulnerability assessment engages the network with full knowledge of its defenses, asset and channels.

The QualysGuard Vulnerability Management software automates the lifecycle of network auditing and vulnerability assessment reporting and remediation tracking according to business risk. QualysGuard utilizes both a centralized vulnerability database and local scanning appliance to provide comprehensive vulnerability assessments of the network.

QualysGuard scans all devices on the Town's network for known and potential vulnerabilities. Reports are generated detailing all of the discovered events and ranking them from Urgent (5) to Minimal (1) in criticality and impact.

The results were used to produce the External Vulnerability Assessment report we received from Compass IT Compliance. The report identified 64 vulnerabilities that existed on our network of which five were given the highest rating of Critical Risk. Many of these vulnerabilities identified required updating the server and switch software to the latest versions. The IT Department was able to fix many of the security issues identified, but some of the issues relating to our firewall could not be fixed because of the age of the equipment.

The IT Department evaluated firewalls from three manufacturers, Cisco, Palo Alto and Fortinet over a period of three months. We decided that Palo Alto was the best suited to address the Town's external security needs.

The original design for our network has one firewall at the Flynn Building in which all of our network internet traffic flowed through. We also have two internet service providers (ISP) at the Flynn Building, Comcast and Verizon FiOS. These connections were setup so that all incoming and external internet traffic went through the FiOS connection. If FiOS was not available, the internet traffic would go through our Comcast ISP. We have setup failover DNS with our managed DNS provider DYN. The failover setup monitors our Website, VPN and Email and if any of those external IPs do not respond the system would failover to the corresponding Comcast external IP until the connection issue was resolved. This ensured that our primary external applications would still be available if our primary ISP connection went down.

During our three-month evaluation period, we created a new a new firewall security design for the Town. The new design consists of two firewalls one at the Flynn Building and the other at the Police Station. The firewalls would be setup as a highly available (HA) pair, in an Active/Passive deployment. If the primary firewall at the Flynn building fails, the traffic will automatically fail to the secondary firewall located at the Police Station providing maximum availability. Dark single-mode fiber will connect to each firewall providing the HA connection between the two firewalls. The internet ISPs used by the Town will be added to separate VLANs that will connect to the primary and secondary firewalls. Combining these resources will increase our internet bandwidth for maximum speed and performance. Having two of the ISPs, FLComcast and FLFiOS in the Flynn building and the other, POFiOS at the Police Station gives us the ability to survive a building wide catastrophe and still have internet access. The Dyn DNS management service will be used for external IP failover, but will be modified to account for the addition of the POFiOS ISP.

We have purchased two firewalls for our Intrusion Prevention System (IPS) service as well as adding subscriptions for Threat Prevention, URL Filtering, Wildfire and GlobalProtect.

Below is a short description of these subscription modules:

Threat Prevention

The Threat Prevention subscription adds integrated protection against network-borne threats, including exploits, malware, command and control traffic, and a variety of hacking tools, through IPS functionality and stream-based blocking of millions of known malware samples.

URL Filtering

URL Filtering provides us with granular, user-based controls over Web activity through URL categories and customizable white- and black-lists, as well as protection from Web-borne threats through malicious categories like “malware” and “phishing.”

WildFire

The WildFire subscription actively analyzes unknown threats, including malware, websites, and command and control traffic, and delivers automatically created protections and intelligence back to subscribed firewalls all over the world for proactive global prevention.

GlobalProtect

GlobalProtect extends the protection of our firewall to endpoints both inside and outside of the Town’s network, delivering consistent security to users in all locations. Mobile devices can use GlobalProtect apps for iOS and Android to connect to the Town’s firewall, and we can apply the state of the endpoint device as part of the context for security policy using the Host Information Profile (HIP). GlobalProtect subscriptions can also be deployed internally to protect local and wireless networks users.

The upgrade to a next-generation firewall allows us to classify all traffic, including encrypted traffic, based on application, application function, user and content. We can now create comprehensive, precise security policies, resulting in safe enablement of applications. This lets only authorized users run sanctioned applications, greatly reducing the possibility of cyber-attacks on our network.

The Town has been soliciting proposals from vendors to assist the IT department with the implementation of the new firewalls. We are hoping to select the vendor within the next couple of weeks. We should have the firewall implementation completed by January of 2018.

Expenses

$4,800	Compass IT Compliance	External Vulnerability Assessment
$42,036	Presidio Networked Solutions	(2) Firewalls with Threat Prevention, URL Filtering, Wildfire, Global Protect and Premium Support.
$10,000	Estimate	Implementation of the Firewall equipment and design.
$56,836	**Total**	
$10,000	**Funded by the Community Compact Cabinet**	
$46,836	**Funded by the Town of Sudbury**	