

Dear Superintendent Gilbert,

Thank you for giving me the opportunity to present to the Administrative Cabinet this past Wednesday, October 2nd about the challenges facing the Technology Department this year. As I mentioned in the presentation, the risk of a cybersecurity incident is a rapidly growing vulnerability for K-12 schools. Almost 700 school districts in the last three years have publicly reported cyber security incidents including ransomware attack. In 2019, Connecticut had seven school districts publicly reporting incidents, but as I mentioned, many others have quietly dealt with issues, specifically ransomware. These types of virus infections have lasting effects, and remediation can last months, if not longer impacting daily use of the computer networks such as teachers accessing their laptops and conducting the daily business of the school such as students being unable to buy lunches, teachers unable to use their smartboards, the Business Office unable to process requisitions or payroll.

During my presentation I mentioned that since my budget proposal in October of 2018, the cybersecurity landscape impacting schools has drastically changed. Because of this I have spent the last ten months creating a Disaster Recovery and Continuity Plan for the Technology Department. This is a first step in creating a plan that deals with physical and digital catastrophes within our network, and notes areas where we still are vulnerable. The three most vulnerable areas are availability of antivirus/malware protection for all computers, a secure data backup and recovery solution, and professional development for all staff.

The solutions, with quotes, that I have found to address these vulnerabilities are:

- Malware/Antivirus Protection - \$6,500/ Annually (Malwarebytes)
- DNS Protection - \$11,000/ 1st yr. - \$6,000/ Annually (Cisco Umbrella)
- Data Backup - \$21,530.00 (Unitrends)

I am grateful the administrative team has decided to add the Digital Security and Protection module to GCN online training this year for all members of the Woodbridge School District. This is a good first step in training staff. I encourage finding additional times through the year to further bolster our staff's digital awareness.

I am continuing to speak with vendors and colleagues in other districts to find the most comprehensive solution for our district, digital resources, and digital security. The solutions I have mentioned, as well as other cybersecurity measures, will be included in my budget request for 2020-2021. There may be possible changes in vendors for cost effectiveness.

The threat of a cybersecurity incident is unfortunately very real. It would only take the click of a mouse to cause catastrophic damage. It is crucial we take immediate action to address our existing vulnerabilities while making plans to limit future exposure.

I look forward to continuing the conversation,

James Crawford  
Technology Coordinator