

Update on WPS computer security

9 January, 2016

To: Wayland School Committee
41 Cochituate Road
Wayland, MA 01778

Dear members of the Wayland School Committee:

As you prepare the new WPS budget, there are seven computer security issues you should be aware of:

1. Security updates missing from WPS computers – again

Remember when we discovered last April that hundreds of WPS computers were running old versions of Mac OS? This was a major security issue. The School Committee took quick action and leased ~200 new laptops to replace old ones that could not be upgraded, and Leisha Simon's team updated all WPS Macs over the summer.

Believe it or not, we discovered at the end of November that over 1,700 WPS computers were again running outdated versions of Mac OS – at least two revs and months behind Apple's releases of major security patches. Vulnerable Macs were being used by teachers and departments that deal with very confidential student and staff information, e.g. SPED, Health & Wellness, Guidance, school principals and Dr. Stein's office. All of the laptops used by WHS students were also vulnerable. Here are the details:

- **OS X security patches:** Each update for Mac OS X fixes dozens of major security flaws, similar to the Patch Tuesday security updates from Microsoft. Here were release dates as of November, 2015:
 - ▶ 10.10.3: 8 April
 - ▶ 10.10.4: 30 June
 - ▶ 10.10.5: 13 August
 - ▶ 10.11: 30 September
- **In November, 2015, how many WPS Macs were running an old version of OS X at least 2 revs back, missing dozens of security patches?**
 - ✓ **1,651** Macs used by the main office, school principals, SPED, Health and Wellness and most teachers were running 10.10.4 – 4 months old.
 - ✓ **70** Macs used by Guidance, SPED, the main office and teachers were running an even older version: 10.10.3 – 7 months old.

- **How significant is this problem?** As we noted last April, Apple releases major security updates every ~60 days. (*Copies of two Apple update notes are attached.*) The minute an update is published, all of the details about the matching security vulnerabilities are public, which gives hackers a clear roadmap for attacks. This means that updates must be installed as fast as possible, *within a few days* after release from Apple. This is a standard computer management / security process, also recommended for schools by the US Department of Education.
- **Why were Apple updates delayed for months at WPS?** The WPS IT team was still not using their Casper management system to automatically deploy Mac OS and software updates – even though this is one of Casper’s key functions, *specifically recommended* by the manufacturer (JAMF). We met with Leisha Simon and Dr. Stein and tried to find out why this basic problem recurred. We did not receive a clear answer.
- ▶ **What does the Wayland School Committee need to do?**
Instruct Leisha Simon and the WPS IT team to use Casper as the manufacturer intended, to automatically deploy all security patches *within a few days* after Apple releases them. Time is of the essence.

2. Casper is an incomplete, interim solution

WPS now has a large network with ~1,700 ‘endpoints’ with Mac, Windows and Chromebook computers -- similar to a large corporation. Casper *cannot* manage Windows or Chromebook computers, and cannot alert WPS IT to new or missing security patches.

WPS security needs are also very different from the Town of Wayland, which is shifting to ‘virtual’ Windows terminals that are easy to manage from a central server. WPS cannot depend on whatever the Town of Wayland implements.

WPS needs a more powerful ‘endpoint’ management system that can manage all of the Mac, Windows and Chromebook computers – from one efficient screen. This will significantly improve security and reduce IT management costs. That is why corporations buy endpoint security systems – to cut costs and risk.

There are a number of recognized vendors and products. We provided information to Dr. Stein on the Dell Kace solution, which is one of the least expensive and easiest to use.

▶ **What does the Wayland School Committee need to do?**

Add \$70,000 in the new budget to cover the first-year cost for system implementation. Ongoing costs will be approximately \$30K to \$60K annually, depending on the vendor and services WPS selects. Immediately launch an RFP for solutions from leading vendors. We would be happy to help.

You may be wondering, “Can this wait till next year?” No. Any organization with thousands of Macs, Windows and Chromebook computers needs a system to automate management and security.

To continue with a broken, manual process would be negligent and expose Wayland and WPS to costly liability in the event of a data breach. Wayland taxpayers would foot the bill. As Wayland parents, we do not want our families’ confidential data to be hacked so easily.

- **WPS can also terminate the license for Casper**, which will become redundant after the new endpoint system is installed. This will reduce the total annual cost by ~\$30K.
- **Can WPS depend on the Town to fund this solution?** During the previous meeting, Dr. Stein apparently noted that no security upgrades were included in his new WPS budget because the Town is going to respond to the McGladrey report. I met with Paul in December and we discussed WPS' need for an endpoint management / security product (which includes patch management), which the Town does not need because they are shifting to virtual Windows machines.

I also told Paul that I spoke with Brian Keveny, the Town Finance Director, who mentioned that the Town was looking to the School to pick up their share of the tab for computer security upgrades. Paul and I also discussed how WPS could terminate the Casper license to save ~\$30K per year, which would offset some of the cost.

▶ **What does the Wayland School Committee need to do?**

Make sure Paul Stein’s new WPS budget includes money for an endpoint management / security system, unless the Town confirms that they are going to pay for it -- which seems unlikely.

- **Monthly compliance reports:** You should not have to read another letter about missing security patches, and we should not have to write one. Monthly status reports are needed to make sure security patches are installed.

▶ **What does the Wayland School Committee need to do?**

Request monthly reports from Dr. Stein and Leisha Simon, showing the status of each WPS computer. For now, this can be created easily from the Casper system for every WPS Mac, and WSUS (Windows Server Update Services) for every Windows computer. Nothing needs to be purchased or installed, and this will take only a few minutes to create.

The monthly reports should include these fields:

Computer name, make, model, serial number (needed to check the specs), operating system version, date purchased, CPU, RAM, school and department

3. No data encryption

We also found that WPS did not implement basic data encryption for Mac and Windows computers across the district. Again, this includes teachers and departments that handle very confidential data, e.g. SPED, Guidance, Health & Wellness, principals and Dr. Stein's office. All of the laptops used by WHS students were also vulnerable.

The good news? Nothing needs to be purchased. Disk encryption is a basic function built into Mac OS X and Windows, and simply needs to be 'turned on' by WPS IT. This can be completely automatic; WPS IT staff do not need to manually 'install' or 'configure' anything, computer by computer.

Disk encryption automatically protects everything stored on a laptop or desktop in case it is lost or stolen; this is a standard step in organizations that handle confidential data – like WPS. The US Department of Education also recommends data encryption as a standard practice for schools.

Why hasn't WPS IT implemented encryption? Leisha Simon said, "I would prefer encryption not be necessary". According to government regulations and DOE guidance, however, encryption is a standard -- not a preference. Implementation costs will be minimal using existing tools.

► **What does the Wayland School Committee need to do?**

Ask Dr. Stein and Ms. Simon to present a plan by 15 February to implement disk encryption on all WPS Mac and Windows computers -- covering management, teachers, staff and students -- with completion by 31 March.

Like endpoint security, to let this basic step slide would be negligent and expose Wayland and WPS to unnecessary liability in the event of a data breach. Again, the cost would be paid by Wayland taxpayers and Wayland families would be harmed by the loss of their confidential data.

Legal note: Confidential personal, education and healthcare data held by WPS is covered by Commonwealth and Federal law and regulation, e.g. FIRPA and HIPAA. If an organization implements data encryption, this provides a regulatory "safe harbor" and defense in civil cases. Lack of data encryption, which is recommended by Commonwealth, DOE and Federal statutes and regulations, would create an obvious weakness and source of liability for Wayland and WPS.

4. LanSchool monitoring of student computer use

WPS installed the LanSchool system which can record student communications, the websites they visit, etc. We asked Dr. Stein and Leisha Simon if it is being used generally to record student communications. Dr. Stein and Ms. Simon both said, "No, LanSchool monitoring is used only if there is a problem."

So we gave them a document in December that lists LanSchool settings, and asked them to record how this system is setup. A copy is attached for your review. So far, we have not received a response. Wayland families, the School Committee and teachers should know exactly how this system is being used.

We were also told that WPS *does not have a basic privacy policy* or procedure in place to determine and document how and when LanSchool monitoring should be used if a "problem" occurs, how recorded student data is stored, who can view it, how parents are notified and how parents / students can request copies and corrections as required by FIRPA. (WPS is now working on a policy.)

Last but not least, LanSchool is very insecure. It is easy for students to take control as a "teacher" and monitor other students. The data that LanSchool collects is also stored with a very weak 'encryption' scheme that is trivial to hack. We sent Dr. Stain and Leisha Simon this YouTube link that explains how to take control of LanSchool, one of many examples:

https://www.youtube.com/watch?v=AG-m_G6O5Qo

Wayland High School students know how to login to LanSchool and observe other students, play pranks on them, connect to the Teacher's WiFi network, etc. We sent all of this info to Dr. Stein and Leisha Simon. Paul was very pleasant and professional when we met. We received no response, however.

► **What does the Wayland School Committee need to do?**

- Ask Dr. Stein to provide the document showing how LanSchool has been configured and used.
- Follow up with Dr. Stein to make sure the new WPS security policy is completed quickly – including how a student monitoring system will be used and how resulting data will be managed.
- The LanSchool system is so insecure and open to misuse / abuse that you should ask Dr. Stein and WPS IT to uninstall it.
- Computer monitoring ability could be needed if there is a serious safety concern, of course. This is also a common requirement in corporate settings, and a number of well-tested and secure products are available. WPS and the School Committee should issue an RFP for a replacement system. We would be happy to help.

5. Google apps for education – with significant privacy problems

WPS staff use and promote Google apps for education. Google products are attractive, of course, because they are ‘free’. Unfortunately, Google continues to mine private student and teacher data -- and uses it to target product ads, despite previous denials. See:

<http://blogs.wsj.com/digits/2015/12/01/googles-education-service-under-fire-for-privacy-violations/?mod=rss> Technology

<http://www.networkworld.com/article/3011084/security/google-accused-of-tracking-school-kids-after-it-promised-not-to.html>

(A copy of the Electronic Frontier Foundation FTC complaint against Google is also attached for your review.)

We asked Dr. Stein how he intends to deal with this issue. Wayland families need to know that their child’s personal data is not being captured and used.

► **What does the Wayland School Committee need to do?**

Given Google's apparent violation of their own privacy policy, the School Committee should discontinue the use and promotion of Google education apps in Wayland Schools – until this recurring problem is resolved.

6. Outsource WPS computer management and security

McGladrey recommended outsourced IT management services for the Town of Wayland. This would be a smart move for WPS as well.

► **What does the Wayland School Committee need to do?**

Draft an RFP and hire a firm that specializes in networks of this size, with a diverse base of Mac, Windows and Chromebook computers. Let them manage WPS IT infrastructure – and let WPS staff focus on education. This is a common approach, to improve IT operations and reduce costs.

7. No insurance coverage for data breaches, tax dollars or people

We contacted Nan Balmer’s office to see if Wayland purchased more insurance coverage following the hacking attacks last January. Here is the reply we received from John Senchyshen:

“You are correct. Wayland would need to apply for a separate policy for coverage against data breaches, etc. MIIA does not include coverage in their policies for any municipalities for data breaches.”

What does this mean?

(A) Wayland taxpayers are on the hook for all of the costs in the event of a data breach at WPS. The average for 1 incident with a not-for-profit organization like WPS = \$1.4 million.

(B) There is apparently no insurance protection for data breaches and related lawsuits that covers elected, appointed or hired Wayland or WPS officials and employees who may be named in a civil suit, including members of the Wayland School Committee and Board of Selectmen.

► **What does the Wayland School Committee need to do?**

Ask Nan Balmer to determine how much additional insurance would cost, to protect Wayland taxpayers – and make sure this cost is added to the new Town / School budget. Also press Ms. Balmer and the BoS for *much* faster implementation of the IT upgrades recommended by the IT consultants that Wayland hired: McGladrey and McCann. The glacial pace over the past year only increased the risk – and creates an easy case for opposing attorneys if Wayland is sued due to a data breach.

Why are computer security upgrades particularly urgent for WPS?

After multiple successful attacks on the Wayland network last January, hackers worldwide know that Wayland is a high income town with poor IT security.

If hackers test Wayland's network again, they will find that standard security systems have not been installed, despite the attacks. If you were a hacker, would Wayland look like a prime target?

Please let us know if you have any questions. A number of us are happy to volunteer to help WPS solve these problems.

Aina Lagor

Mark Hays

Kaat Vander Straeten

Kade Crockford

Alison Macrina, Library Freedom Project

Karl Klapper

CC: Wayland Board of Selectmen, Finance Committee, Dr. Paul Stein, Nan Balmer, WTA and public media