

# Network/Data Security



Presented by Serhiy Morhun, Manager of IT  
2-06-2017

# Security/privacy challenges

- Technology evolves rapidly and so do the security threats.
- There are no “one size fits all” solutions. Every implementation is a balance between security, privacy and functionality.
- Often times privacy measures could be detrimental to the overall security of the network and a lot of security measures would invade the end user’s privacy.
- Both privacy and security measures can reduce the ease of use and functionality of your systems.

# EDU vs Business - Unique Challenges

A similar sized organization in EDU would normally have:

- More network users (staff + students)
- More client devices to secure (1:1)
- Lower budget
- Our end product cannot be measured financially (cost benefit is impossible)

In EDU, we do not get to pre-screen or select most of our network users and we get the widest range of skills among them. Most potential hackers in EDU are already inside our network.

# Protect - Detect - Respond

It is impossible to completely protect your network from security breaches.

**“Protect”** - set of security measures (tools, procedures and policies) to make it as hard as possible for an unauthorized person to access your network or data.

**“Detect”** - set of monitoring measures to keep track of network activity and alert IT team to any potential indicators of breaches or unauthorized activity.

**“Respond”** - set of response procedures to investigate potential threats, stop malicious activity in progress, analyze incidents to improve future security.

# RPS network/data security

We employ a comprehensive set of security measures and tools following the best practices developed over time in collaboration with other schools and districts as well as our security vendors.

- Firewall for controlled access to internal resources with edge antivirus, botnet protection, etc.
- Segmented network to isolate “guest” devices from internal resources
- Access control measures in every data system to limit access
- Secure encrypted web access to our data systems
- Client antivirus on all PC and MAC computers, etc.
- Web content filtering

# Into the Cloud

G Suite For Education (GSFE) - formerly Google Apps For Education (GAFE)

2013 - GAFE was introduced at RPS.

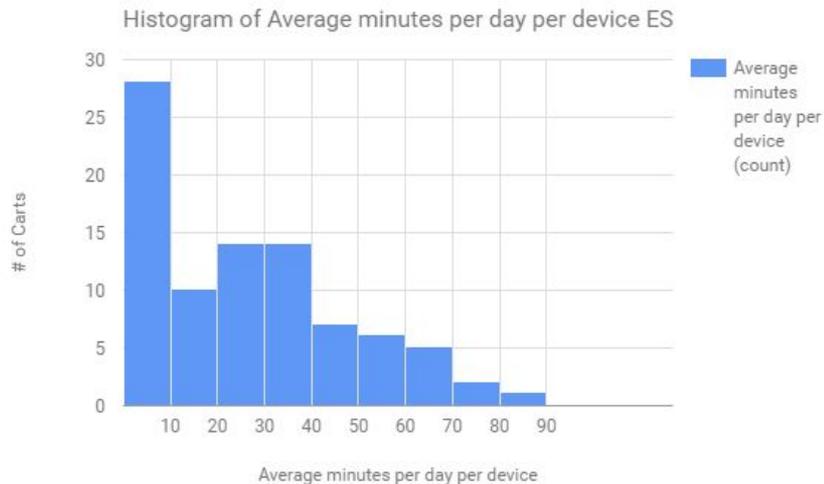
2014 - 1:1 program with Chromebooks at RHS.

2015 - 1:1 program with Chromebooks at BF & GW. Google Classroom introduced.

2016 - 1:1 Chromebook program effectively covers students in grades 2-12. Grades 2-5 classrooms utilize classroom carts, grades 6-12 take home.

# Chromebook usage

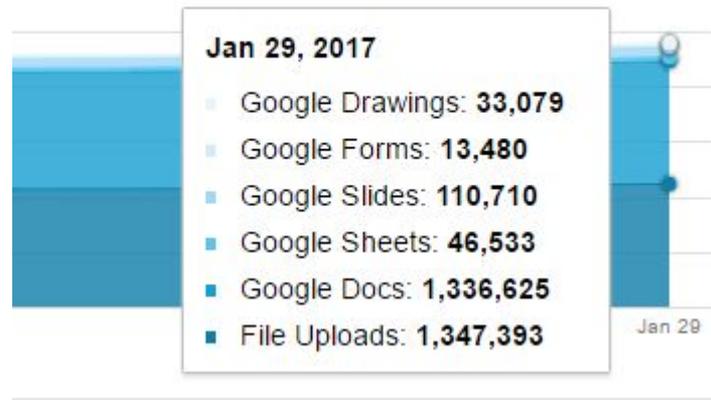
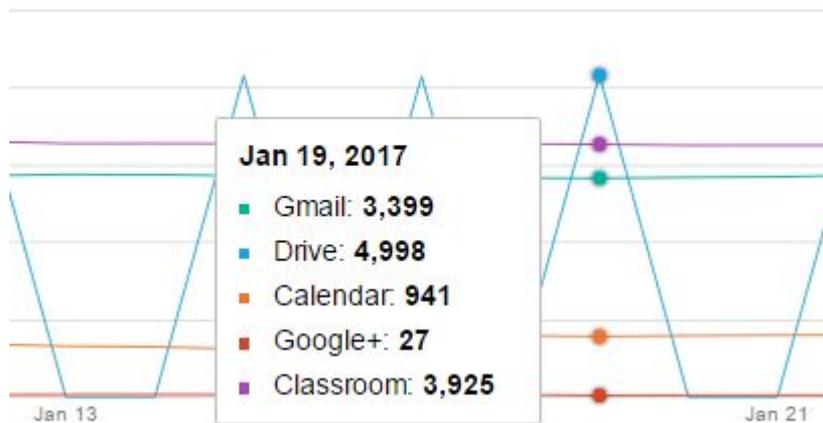
15 day average calculated Chromebook use (January 25)



|  |     |
|--|-----|
| /Students/High School/RHS/RHS Grade 10 | 93  |
| /Students/High School/RHS/RHS Grade 11 | 80  |
| /Students/High School/RHS/RHS Grade 12 | 84  |
| /Students/High School/RHS/RHS Grade 9  | 117 |
| /Students/Middle Schools/BF/BF Grade 6 | 72  |
| /Students/Middle Schools/BF/BF Grade 7 | 84  |
| /Students/Middle Schools/BF/BF Grade 8 | 74  |
| /Students/Middle Schools/GW/GW Grade 6 | 83  |
| /Students/Middle Schools/GW/GW Grade 7 | 82  |
| /Students/Middle Schools/GW/GW Grade 8 | 88  |

# GSEE usage

About 7,200 provisioned user accounts. Over 6,100 chromebook devices.



# GSEE security/privacy

We take advantage of Google's industry leading secure Data centers and services. This is the same service being used by Google itself and their paying customers, but with much improved data privacy practices for EDU domain (FERPA compliant).

- G Services and data centers are ISO 27001 certified.
- Logical data separation.
- Encryption of data in transit for all services including Gmail and Drive.
- Signed Student privacy pledge. Limits data collection to only what is required for services. Does not advertise in EDU domains.
- Provides extensive security, administrative and archiving controls to the district.

# Who is in control?

Google provides the service, but they do not own any of our data. They provide management tools for a granular control of the services, usage and data.

- We provision user accounts only with age appropriate services.
- Chromebooks - very secure platform with almost non existent “attack surface”.
- We provision chromebooks to further reduce possibilities of tampering.
- Gmail - comprehensive set of measures to battle spam, phishing and malware. We also maintain content compliance rules to quarantine phishing and keep our staff informed if any phishing campaigns get through.
- Chrome browser - a slew of security features: sandboxing, malware site warning, insecure site warnings, etc.

# Web content filtering

- The Internet is a vast collection of ever changing resources. We have to rely on 3rd party filtering solutions. Filtering is about balance.
- We employ 2 content filtering solutions: Lightspeed & GoGuardian. They are both for education only.
- Lightspeed - content filtering on the network for all and off network for 6-8.
- GoGuardian Admin - students monitoring and partial filtering for 6-12.
- GoGuardian for Teachers - Chromebook activity monitoring and control by teachers while in their classroom.
- Provide additional security by blocking malicious content from the web.
- Very limited number of people have access to collected data.

# Is our network/users/data safe?

- Yes. We employ a comprehensive set of tools and measures to prevent unauthorised and malicious activity, but there is no system that is 100% safe.
- Weakest link - users. No system exists that can control end users.
- “Social engineering” - phishing attacks became very sophisticated.
- Students who are actively trying to bypass our security measures to access their favorite game, blog, chat site will also reduce their own safety.
- That is why we have monitoring tools and response procedures.
- Google provides a whole set of reports and alerts. We also use additional 3rd party tools to monitor our network and Google activities.
- We have a very skilled IT team, but no dedicated security division.

# Robust infrastructure and redundancy

- Robust and reliable network and Internet connection is a must in 1:1 environment and cloud computing.
- We have been preparing our network for a number of years.
- Redundancy has been built in at every level that was not cost prohibitive. Redundant power supplies, storage, networking devices. Secondary Internet connection.
- Our Data Center implementation employs DR solution as well as Data backup.
- We cannot match Google's 99.978% availability, but we are well equipped to deal with outages in a timely manner.

# **One big advantage of EDU over Business**

The most effective security/privacy measure is educating your end users.

We are uniquely qualified for that.