securly://

1:1 device theft in k-12 schools: a survey driven study

tech brief – winter2015 – v1.1

Table of Contents

Background

In our many conversations with IT Admins, the topic of lost or stolen school devices (e.g., Chromebooks, iPads, Android tablets, etc.) is one that occasionally comes up in the discussion. To date, however, we have found that there has been insufficient information to answer questions such as:

- How often are devices lost or stolen?
- Is insurance worth the cost?
- What are the most viable measures to protect against loss and theft?

As we are constantly striving to understand schools' needs when it comes to managing and securing their 1:1 programs, we sought out to find answers to these questions. While we have done a significant amount of research for this study, we are always open to new ideas and feedback.

Survey Methodology

Our survey and interviews were divided into the following groups:

- Anonymous survey of 100 IT Admins, half of whom were Securly customers and the other half were randomly sampled admins who are not affiliated with Securly.
- Interview with Lieutenant Tom Sims of the San Jose Police Department to gain insight into school device theft from the perspective of law enforcement.
- 1-on-1 interviews with twenty customers and prospective customers
- Email exchanges with Google's official Chromebook deployment team

In order for their response to be included in our results, all IT Admins were required to be currently: (1) Employed by a K-12 school or district, and (2) Managing a school 1:1 device program.

Exhibit A: Location of 100 respondents from the US and the UK

The survey questions were as follows:

1. Do you have a 1:1 program at your school?
   [YES / NO]

2. Do you purchase insurance for your 1:1 devices?
   [YES / NO / OPTIONAL OR REQUIRED FOR PARENTS]

3. Per device, what is the annual cost of insurance?

4. Does your insurance cover theft?
   [YES / NO]

5. How often does device theft occur in your school?
   [4-POINT SCALE: 1 = NEVER, 4 = FREQUENTLY]

6. Fill in the blank: "We have 1 device stolen for every _____ devices."

7. How often do your students (as a whole) lose or misplace their school devices? Note: Please disregard whether or not the device is recovered.
   [4-POINT SCALE: 1 = NEVER, 4 = FREQUENTLY]

8. Fill in the blank: "We have 1 device lost or misplaced for every _____ devices."

9. Of the devices that are lost, approximately what percentage is recovered?

10. How desirable are anti-theft technologies built into your Chromebooks/iPads?
    [5-POINT SCALE: 1 = NOT DESIRABLE, 5 = HIGHLY DESIRABLE]

11. Assuming for a moment that loss is more common than theft, what would you look for in an anti-theft solution – location tracking or additionally web-cam captures and keyword logging as well? Please explain.

Survey Results

Of the 100 IT Admins who were surveyed, 96 met the required conditions to be included in the results. The study revealed the following information:

- 58% of all respondents either purchase insurance from school funds or share the responsibility with parents.

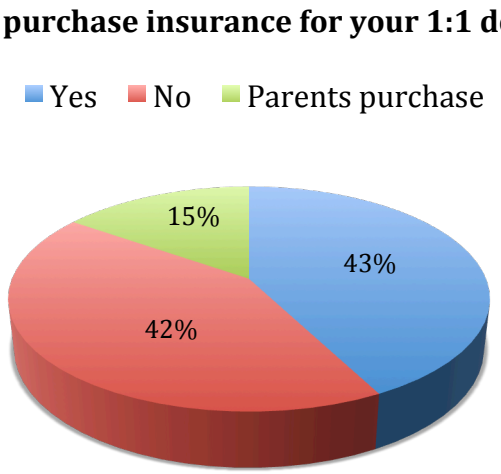


Exhibit B

- For schools that purchase insurance, the average annual cost of insuring one device is $27, with 78% of respondents paying $40 or less per device.

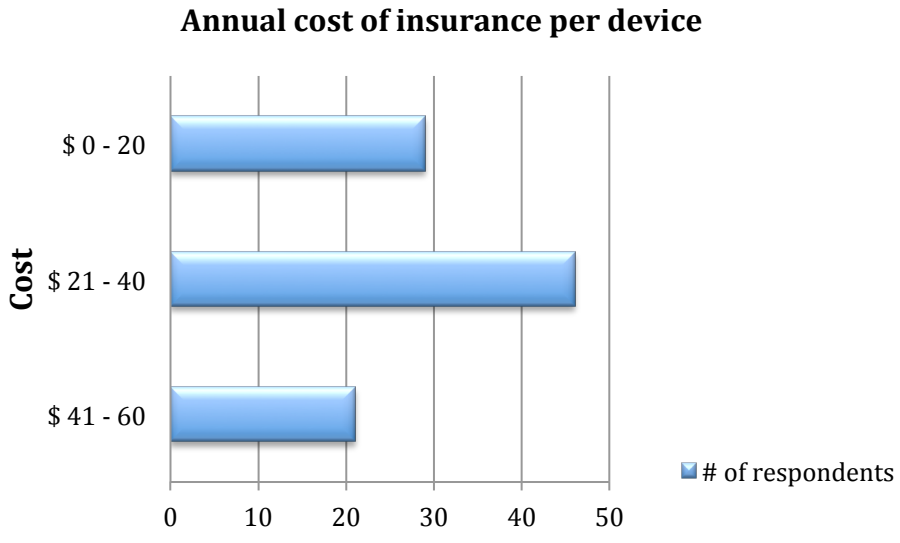


Exhibit C

- 50% of respondents stated that their insurance provider includes coverage for theft. For this group, the average cost of insurance per device was $28, or $2 above the average cost for respondents without theft coverage.

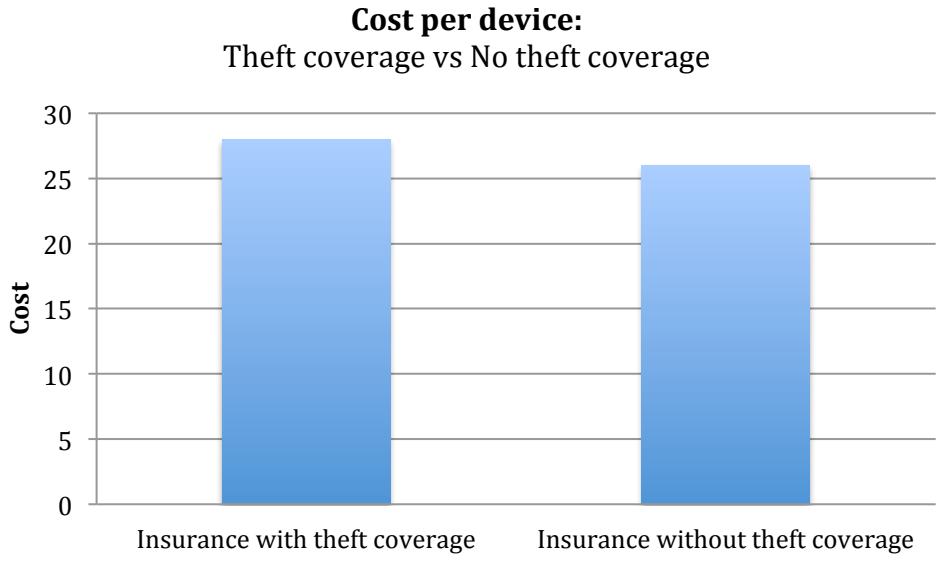


Exhibit D

- 84% of all respondents reported that device theft rarely or never occurs in their school.

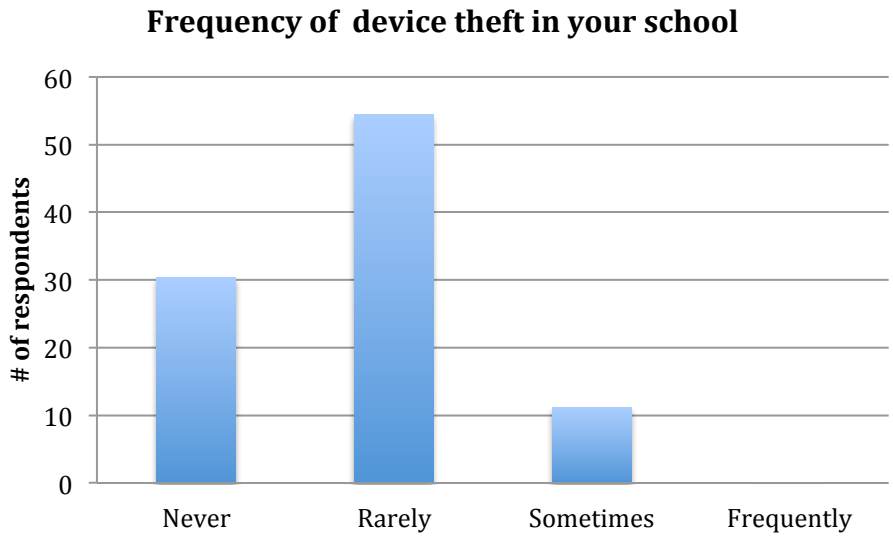


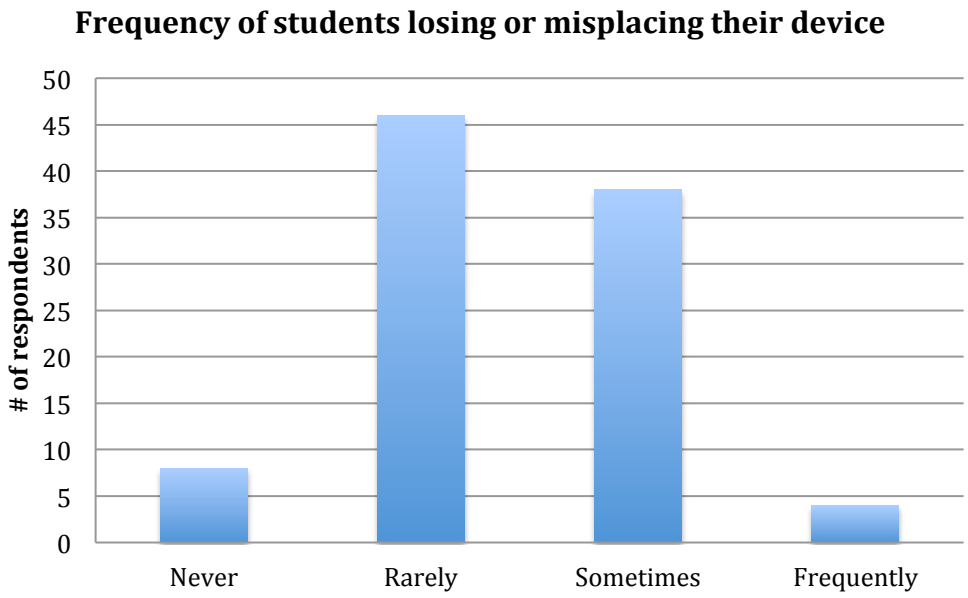
Exhibit E

- On average, schools reported their device theft frequency to be 1 in 700[*]. Assuming that the average cost per device for a combination of iPads and Chromebooks is $400[†], and using the average cost of insurance per device of $27 from the survey, we estimate the break-even point for the insurance investment as follows:

  Assume the school loses 1 in Y devices to theft each year. Then at $27/device for insurance, the school recovers the $400 loss with all Y devices insured. That is, $27xY = $400. Or if Y=15. In other words, to justify the cost of insurance, there must be 1 in 15 devices stolen each year.

  An alternate way of looking at this is that for insurance to be worthwhile, it must be available at a cost of $0.57 (400/700) per device.

- 44% of all respondents reported that students in their school at least sometimes lose or misplace devices



[*] *Actual figure could vary depending on a host of other factors, including school size and setting (e.g., urban, suburban, rural)*

[†] *Assuming an equal number of Chromebooks and iPads across school based on Q3 2014 data: http://www.techrepublic.com/article/chromebooks-leapfrog-ipads-in-us-education-market-for-first-time-heres-why; we also calculated the average retail price of an iPad ($529) and Chromebook ($272) across all models (with the exception of the higher-priced Chromebook Pixel)*

- On average, admins reported that 1 in 230 school devices is lost or misplaced by students. In other words, incidents of missing/lost devices are three times as likely to occur as are incidents of theft. A few respondents acknowledged that the frequency might be even higher than they reported given that it does not reflect temporary loss in individual classrooms, the school library, or other common areas where students bring their devices. For the devices that were lost, respondents reported that they were recovered 68% of the time.

- Despite the admittedly low rates of theft, 79% of all respondents answered that an "anti-theft" solution would be at least fairly desirable

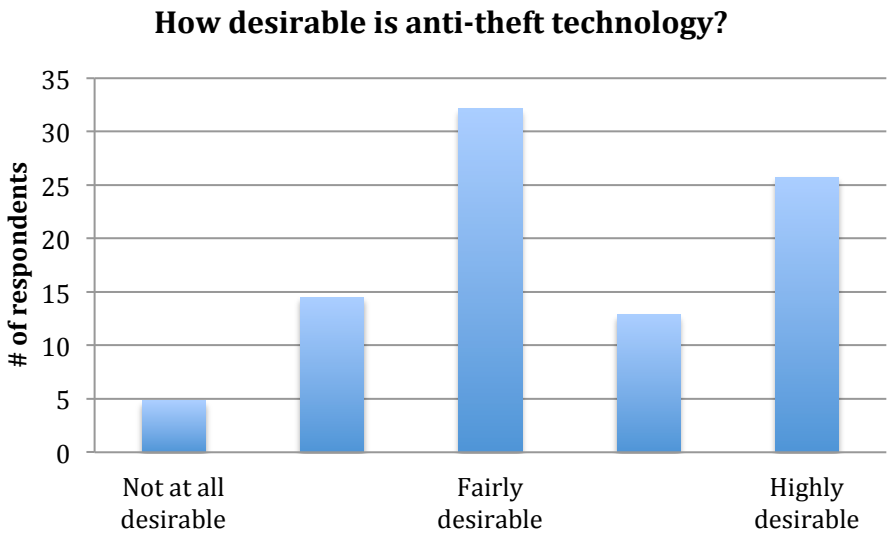


Exhibit F

- To better understand exactly which features were the most appealing to admins, we subsequently asked whether the schools would be interested in any of the following options:
    - **"Anti-loss" or Location tracking** for lost or misplaced devices,
    - **Remote-disable** and remote-wipe for stolen devices, or
    - **"Anti-theft"** features such as remotely taking screenshots or logging keystrokes for stolen devices

The results show that the majority of admins care most about being able to track the location of the device. Randomly selected samples of these comments are shown below in Table A:

Yes, as we are an online school this would allow us to track the location
We do not have a take home program. When we do become a take home program, we will become more interested in this option.
anti-loss as a preventative measure
Location tracking would be fantastic, but as many ISPs report indirectly and the devices don't have GPS, I'm not certain how well it will work.
Yes. Geolocation would be perfectly fine.
Yes, but since any Loss Prevention program or software generally looks for the ip address of the device, it hard to find that if they are within our LAN.
Anti-loss sounds ok.
While we have not yet had any reports of theft, we frequently have students misplace their Chromebook and we would love to have the ability to locate the device.
Any loss is a loss, so physical tracking is a worthwhile pursuit
Yes, and Anti Loss program would cover 99% of our issues
still desire specifically an anti-theft solution
Geo-location tracking would be sufficient. We haven't had any lost or stolen this year, but it would be very beneficial to have this functionality.
Yes, a geo-location tracking would be excellent. The ability to disable the device would also be desirable.
Anti-loss would be suitable.
We need a system that will track a device in school or out. Looking for a device once it is lost or stolen is no good. We basically need to know where it was last either before the battery ran out or the device was factory reset by a thief. It also needs to report location when on standby.
Allowing more information than just geo-location has helped us track down units in other school districts all the way to Mexico. We couldn't recover the one in Mexico but at least we know where it is and that the student was telling the truth that it was stolen.
yes, I just want to be able to track the device if needed, similar to how iPads can be tracked with a Geo location and audio signal options.
These devices are capable of handling the tech required to do this....therefore it makes sense to have it! It will also greatly increase the value of your software. Our school is currently looking into this as we feel it is a needed resource....
anti-loss would be sufficient
Loss is far more useful.
Location tracking would be a huge advantage when students are prone to walking off without their chromebooks...
Geo-tracking is sufficient. But additional features would be nice in the case of actual theft.
anti loss with geo location tracking

Table A

Interview with Law Enforcement

Lieutenant Tom Sims
Division Patrol Commander
San Jose Police Department
San Jose, California

In addition to the school admins we surveyed, we felt it would be insightful to get the perspective of a member of law enforcement on recovering stolen school devices. We sat down with Lieutenant Tom Sims of the San Jose Police Department – which protects over 1 million residents[‡] in the city of San Jose, CA – to get his take on the frequency of stolen school devices as well as the process of recovering them.

Securly: In your estimation, how often does device theft occur in K-12 schools?

Lt. Sims: Given that San Jose is the 10th largest city in the United States, we feel that we're a pretty good breeding ground for these types of statistics. While we do have hundreds if not thousands of residential thefts each year, we don't get a whole lot of reports of school burglaries.

S: Do the police invest time and effort in locating one stolen device or would the report have to consist of numerous stolen devices to pursue?

LS: It depends on the situation. If someone broke into a school and took an iPad, we would certainly go through the same routine as we normally do – come in and look for the point of entry, fingerprints, etc. That being said, with burglaries, the value of the merchandise reported stolen dictates whether the crime is a felony or misdemeanor. So we will invest more resources for a large amount of loss as compared to, for example, if a car was broken into and one iPad was stolen.

S: What is the likelihood that you recover the stolen device(s)?

LS: This is dependent on the amount of evidence. If the thief didn't trigger an alarm or leave things behind, it's unlikely.

S: How helpful would it be for the police to have the ability to use anti-theft tools like logging device keystrokes and remotely taking a picture of the thief?

---

‡ *http://www.sanjoseca.gov*

LS: We find that most thieves don't use the device themselves. It's more likely instead that they pawn it off to a friend. We often hear something like "Bob sold it to me for $50". Thus, we're not overly concerned with *who*; it's more about *where*.

Student Privacy Concerns from the Community

A recurring theme throughout our 1-on-1 interviews with IT admins was the issue of student privacy. Specifically, where do admins feel they should draw the line in their attempts to recover school devices?

What we discovered is that while location tracking is something that admins believe adequately protects a school's investment as well as its students, other anti-theft technology is often perceived as intrusive and in violation of student privacy. In particular, the ability to remotely capture a picture of a device's user was unsettling to most IT admins we interviewed. Keeping in mind that a stolen device is often sold off to someone else, they felt that employing this feature on an unsuspecting individual would be a serious violation of privacy. Moreover, one interviewee in particular pointed out that while the majority of IT admins most certainly do not abuse technology, all it takes is one individual with poor intentions to spy on an unknowing student.

This sentiment has been echoed on various forums and podcasts, one example being John Oliphant's YouTube channel entitled "Practical Chrome":
https://www.youtube.com/watch?v=W4cJzNepJMo#t=40m11s

Google: Remote Disable. No Webcam or Keyword Logging

We have been monitoring Google's own take on anti-theft for a while. Sometime in mid 2014, the developer community noticed Google's foray into location tracking functionality for Chromebooks:

http://www.muktware.com/2014/05/09/soon-will-able-lock-erase-locate-lost-chromebook/

http://www.pcworld.com/article/2153541/google-hints-at-remote-wipe-lock-and-locate-features-for-chromebooks.html

As of January 2015, Google has already introduced the "remote disable" functionality into the admin console: https://support.google.com/chrome/a/answer/3523633

Here's a primer on how this functionality works written by Karl Rivers from ClassThink:
http://www.classthink.com/2015/02/05/how-to-deal-with-a-lost-or-stolen-chromebook/

We have tested this functionality extensively, and find it extremely well done by Google:

- A stolen Chromebook can be disabled at any point of time after it is reported stolen

- The admin can see a history of login activity on that device to see if users from outside the school accessed the device

- The developer mode itself gets locked out preventing the thief from attempting to install Ubuntu or other operating system on the device

- Even if the thief stays completely offline to enter the developer mode, wipes the device clean, and loads the Chrome OS in offline mode, if at any point of time in the future the device is taken online (e.g. to download the tools to install Ubuntu on it or if its sold off to other students), the device immediately gets locked out

With this simple but effective solution, the Chromebook essentially becomes useless to the thief and deters additional thefts of Chromebooks.

Finally, we asked the Google Chromebook team whether there were any plans for location tracking, remote web-cam, and keyword/URL logging features for the device, and we were told that for privacy reasons, Google has decided not to implement any of these at this time.

Summary & Recommendations

After reviewing our survey data of 100 IT admins, 1-on-1 interviews with the San Jose Police Department and several IT admins, and studying Google's own response to device theft, we have arrived at the following conclusions:

1. Device theft in K-12 schools is rare; loss is far more common

It is three times as likely that a school device will be lost or misplaced as opposed to stolen. Using estimates of annual theft in San Jose schools provided by Lieutenant Sims, we extrapolated to the rest of US school districts and found that, on average, each district can expect to experience an incidence of device theft 0.34 times a year.[§]

While burglaries in schools do certainly occur, these are not usually for 1:1 devices that go home with kids, but rather thefts of devices that stay in school such as servers, printers, projectors etc. The theft in such cases is usually not that of one device, but of many devices in one burglary. Police invest resources in pursuing only large volume or incidence of thefts and not the theft of a single iPad. Further, even for larger thefts, the police are primarily interested in "where", and not "who" as the devices are often quickly sold off to the street.

[§] *There are approximately 18 thefts/year for San Jose's 307 schools, or 0.06 thefts/school/year. Applying this number to the rest of the US school districts, which on average consist of 5.8 schools (from NCES data), the total number of thefts per year for the average US school district is 0.06*5.8 = 0.34.*

2. For lost (misplaced) devices, use location tracking technology. For stolen devices, report the incident to the authorities.
   An overwhelming majority of survey respondents and interviewees asserted that the single most important piece of information needed to retrieve devices is their location. If students losing or misplacing their devices is a valid concern, and your district policy allows this, we would recommend using a technology that allows you to track the location of all of your devices.

   Given the uncertainty of the type of criminal you may be dealing with, incidents of theft are best left to the local authorities. That said, the police could certainly make use of location tracking technology should schools choose to use it.

3. Include coverage for theft if purchasing insurance
   Ultimately, schools may decide that purchasing insurance is the route they would like to take. As we have found from the survey results, the difference in cost between insurance programs that include theft coverage versus those that do not is negligible. Thus, if schools do indeed decide to purchase insurance, it would be prudent to ensure that device theft is covered by their insurance plan. What would also be important to bear in mind is that insurance pays for itself only in cases with a large amount of loss.

   For schools employing 1:1 programs in which students take devices home, we recommend that the parents, if able, absorb the cost of insuring the device.

4. For Chromebooks, Google's remote-disable feature is an "uncreepy" and safe way to deal with theft
   There are privacy issues with web-cam and keyword logging, just as there are safety concerns over attempting to recover stolen devices from thieves through location tracking. However, Google's solution of essentially "bricking" the Chromebooks and leaving a "Please return this property at the following address" message on the bricked device, in our minds, is the best response to device theft that eliminates privacy and safety concerns, deters any additional Chromebook thefts and significantly increases the likelihood of the devices being returned to the schools.

Once again, please feel free to help us better understand schools' needs if the survey and our conclusions don't seem to accurately capture the community's take on device theft.

Also check out our other whitepapers on Best Practices for your 1:1 Deployments and Best Practices for your Chromebook 1:1 Deployments.

Please write to us on Twitter (@SecurlyInc) or Google+.