SCANTRON

Five Faulty Assumptions Small and Medium School Districts Make About IT

If you manage IT for a small or medium district, you probably have a broad list of things to worry about and a small, shared staff to work with. Overloaded district IT teams often have to make difficult choices between urgent or new projects and just keeping district IT operational. It's easy to relegate certain tasks to the "when we get time" box. However, there are a few IT-related assumptions that, left unchecked, can turn into urgent crises.

Do any of these statements sound familiar?

1. *Vendors are practically giving schools devices, so adopting a 1:1 strategy will be easy*
2. *We're too small for anyone to want our district data. We don't need to spend money or time on cybersecurity.*
3. *We can take care of things ourselves.*
4. *We haven't had a problem for years. Why should we worry about it now?*
5. *It's too expensive.*

Even if you think you're covered, you may be surprised to discover that there's a cost or security exposure.

Assumption #1: Vendors are practically giving schools devices, so adopting a 1:1 strategy will be cheap and easy.

Your IT team may not be making this assumption, but are your administrators? Many large tech companies are making laptops, tablets, and other devices available to schools at a very low cost per device. This leads to the idea that you can measure the value of a device based solely on its replacement cost.

FACT: The device cost itself is a small percentage of any 1:1 initiative.

Further, the devices themselves may be inexpensive, but any set up or consulting needed does not come for free. At a minimum, you need to do the following for any new device:

- Install and update operating systems on the devices
- Install and setup network device-management tools on your server(s)
- Make sure the new devices are enabled in your network management tools

- Set up and enable security
- Import default preferences
- Map drives and printers
- Install default educational applications

These processes can take up to an entire day per device (depending on your team's experience and the availability of device-deployment automation). The setup and configuration effort's true, rolled-up cost includes considerations such as labor, missed educational opportunities, delays in either the rollout or day-to-day tasks, and more. This true cost might exceed the cost of managed IT services for an entire year.

Further, even if your team is comfortable rolling out such initiatives themselves, working with a managed IT provider extends your team's capacity, which can significantly increase the speed of your rollout.

Assumption #2: We're too small for anyone to want our district data. We don't need to spend money or time on cybersecurity.

It's easy to look at the total size of your district and think, "We have nothing to steal. We're not a target. I'm sure we're under the radar."

FACT: School districts suffered at least 348 reported attacks in 2019[1], tripling 2018's reported attacks[2], and that number continues to grow.

Common Attacks

- Web-based (browser)
- Phishing or social engineering
- General malware
- SQL injection
- Compromised or stolen device
- Denial of service
- Advanced malware / zero day attack
- Malicious insider
- Cross-site scripting
- Ransomware

Source: "Cyber Attack - What Are Common Cyberthreats?" Cisco, Cisco, 30 Mar. 2020, www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~types-of-cyber-attacks.

The New York Times reports that districts and schools are a very interesting target for hackers because they often lack staff members dedicated to cybersecurity. "Nearly two-thirds of school

[1] Levin, Douglas. "K-12 Cybersecurity 2019 Year in Review." *The K12 Cybersecurity Resource Center*, The K12 Cybersecurity Resource Center, 2019, k12cybersecure.com/year-in-review/2019-incidents/.

[2] Cisomag. "Number of Student Data Breaches Tripled in 2019: Report." *CISO MAG | Cyber Security Magazine*, CISO MAG, 28 Feb. 2020, www.cisomag.com/ransomware-attacks-and-data-breaches-on-u-s-schools-and-colleges-triple-in-2019/.

districts in the United States serve fewer than 2,500 students, and many do not have a staff member dedicated solely to cybersecurity, according to Keith R. Krueger, the chief executive of the Consortium for School Networking, a group that represents technology employees at primary and secondary schools."[3] Due to this constraint, hackers see schools as a "soft target."

Hackers employ a wide variety of methods to attack data sources, including email phishing, denial of service, ransomware, and others. Districts large and small are under attack, as you can see by visiting the K–12 Cybersecurity Resource Center's Cyber Incident map.

Depending on the infection, an attack could require a total rebuild of your network. This means spending days to resolve the situation and recover your data if possible. A malware attack could be worse: the mind behind it could encrypt all of your data and demand a costly "ransom" to return it to you.

Here's what you have that cybercriminals want:

1. Educator and student email addresses, physical addresses, and other personal data
2. Phone numbers
3. Billing addresses
4. Asset information
5. Academic records and standings
6. Direct-deposit/online payroll banking data for staff, and payment routing data vendors

If someone walked through the door and asked for this information, you would quickly escort them out. However, without dedicated cybersecurity staff your "cyberdoor" is wide open. This is why you need to actively manage IT cybersecurity. Security costs a degree of effort and money, but it is far less costly than several days' worth of downtime, a total data disaster, or the cost of implementing any remedial actions required via Family Educational Rights and Privacy Act (FERPA) enforcement. Working with a managed security provider can take this effort off your already crowded plate.

Assumption #3: We can take care of things ourselves.

Let's say you don't have a 1:1 student device initiative—in other words, all district computers are in controlled labs, or on teacher and office staff desks. You trust your educators and students to be careful, and all devices have malware checkers installed. All your key applications and data are backed up in the cloud and/or offsite. The network is secured and you patch once a month

[3] Bogel-Burroughs, Nicholas. "Hackers' Latest Target: School Districts." The New York Times, The New York Times, 28 July 2019, www.nytimes.com/2019/07/28/us/hacker-school-cybersecurity.html.

or whenever you think about it. You can map new devices and troubleshoot as needs arise. No big deal, right?

FACT: What you don't know about IT will eventually hurt you.

Every day, millions of automated scripts are running throughout the internet looking for access points. Email attachments, browser exploits, real and fake software updates, very convincing phishing campaigns, "free" downloads with default installation settings for malware and bloatware, and increasingly, social media exploits.

49% of data security breaches occur due to human error or system failure, rather than malicious intent.

On a properly managed device, an IT support system scans thousands of data points every day looking for errors, countless entries in system logs, virus and malware alerts, operating system updates, third-party utility updates, and system capacity.

If an error goes unnoticed on an improperly managed device, it could result in a crashed system instead of a proactive fix. It is impractical for an individual person or even a small team to stay up-to-date or to be proactive for every device, given the volume of logs and updates that are generated every day.

Automation, monitoring, and reliable response practices are a must. A managed IT provider can help you set up and monitor tracking and define policies and a response plan.

Assumption #4: We haven't had a problem for years (if ever). Why should we worry about it now?

This rationale pops up frequently when users raising it were active during the Y2K crisis. When all the dust settled, conventional wisdom held that the issue was mostly hype and we shouldn't have made such a fuss. That sentiment persists to the present day.

FACT: There is an exponentially greater number of threats today.

The Y2K crisis was in all likelihood a genuine threat, because the built-in date flaw was present in almost every type of software, in many solid-state devices, in every industry vertical, and especially so in government applications. Fortunately, high awareness and proactive effort by expert IT staff paid off with minimal failures.

Two decades later, systems are increasingly complex, there are more regulations to be aware of, your data is more critical than ever, and the burden of anticipating and mitigating threats is far heavier. Further, cyberattackers are not getting dumber. Quite the opposite—it requires

vigilance to ensure that your cybersecurity comes up with solutions at least as fast as hackers come up with attacks.

Not only do you need the insurance, but also examining your security and IT management procedures can have the side effect of improving IT performance—something that districts that anticipated and headed off the “millennium bug” realized.

Assumption #5: Outsourcing IT help is too expensive.

Right now, you may be weighing the cost of outsourcing management or extension of IT support against the cost of “doing nothing.” While the cost of a service agreement is a fraction of hiring a full-time dedicated IT administrator, it still might feel like an “optional” expense that could be among the first line items to go.

FACT: Your information technology is a critical asset and represents the cost of operating a district. It is the lever that can either stunt your growth if poorly managed, or allow you to multiply your efforts beyond your current capacity if used properly.

It may seem trite, but the question shouldn’t be, “Can I afford managed IT?” but rather, “Can I afford NOT to have managed IT?” Adding headcount in a district is no easy task—and often you don’t need new full-time staff, you need a little help to smooth out the peaks and valleys of supporting a modern learning environment.

Try scratching out some numbers: what is an hour of downtime worth? As you explore virtual learning options, what might it cost to extend your network to remote learners? What security concerns arise if you’re opening your network to remote learners and educators? Can your district survive a catastrophic data loss? Can you withstand a lawsuit if your network infects another network?

Managed IT services are a proactive way to safeguard your data, your productivity, and your district from unseen threats or normal failures. It is the cost of operating a learning environment—whether on-campus or virtual—today.

Bonus! Assumption #6: Only bigger districts need to keep track of printers and print usage.

One of the most commonly neglected areas of educational office management is printing and copying costs. You look at the small number of multi-function copier-printers combined with a dozen laser desktop printers, perhaps even a handful of inkjets, and think, “This isn’t worth managing.”

SCANTRON®

FACT: Print costs in schools usually represents the second largest operating expense after payroll costs—further, if print and copy devices are networked and store local copies of printed items in their buffer (most do), they are vulnerable to cyberattack.

You probably look closely at every lease you sign and you carefully plan capital projects. You're cautious about screening employee and vendor candidates and you balance expenses and costs against opportunities. Are you missing an opportunity to manage print costs, which could be as high as 3% of your operating budget?

Not only does managing your print volume and operational costs give you good intelligence about where printing is occurring, it can also help you streamline your fleet of printers through better placement, higher utilization, and replacing unreliable devices with reliable ones.

Effective managed print services reduce costly downtime resulting from printer issues. An hour of printer-copier downtime for a 50-teacher district may have a proportionately much bigger impact than an hour of downtime for one school in a 1,000-teacher district.

Ask Scantron for Recommendations

Keep your district running smoothly with a secure, highly performing and highly available IT environment. Contact Scantron to talk about developing an IT strategy that makes sense for your district. Leverage our industry-leading tools, experienced field service technicians, and prompt remote and onsite service capabilities. Learn more at www.scantron.com/k12-managed-it.