Welcome everybody, my name is Joe Gioia, I am an educational technology consultant and today I am going to discuss some of the issues and challenges facing educational technology professionals. As an information technology professional in K-12 education, you have quite a challenge...possibly one of the greatest challenges since the first computers were introduced to your schools. The challenges affecting technology leaders in schools today are numerous, from being an internet policeman patrolling for cyber bulling and network threats to someone who has to think outside the box for creative ways to receive funding due to budget constraints. You are also forced to manage all these issues without enough staff.

These are the four critical challenges I will be discussing in detail today. I must emphasize critical because when any one of them falters whether it be a security breach or not enough staff on hand due to budget cuts, an institutions overall technology is threatened. Although I will bring to light several challenges technology professionals face, it only touches upon those mentioned and by no means qualifies as a complete list. Further research and evaluation is necessary to attain a full appreciation of all the challenges technology professionals face when it comes to technology in education.

The first issue I will talk about is security, which according to the 2008 Current Issues Survey Report, is the number one issue that emerged among colleges and universities. With so much talk of identity theft, hackers and scammers it is hard to do anything on your computer without wondering who could possibly be looking over your shoulder. With so much of our business being conducted over the Internet and on your computer, more is at stake than ever before. It is up to school technology professionals to do all that is in their power to keep school networks safe and secure from intruders and malicious attacks.

There are some fundamental things that can be done to help decrease the risk of your school or university falling victim to an attack. The first thing that should be done is have an up to date antivirus program installed on all the machines in the district. Anti-virus software protects your computer from viruses that are downloaded without your knowledge. These viruses are difficult to detect at first glance and could be missed and allowed to destroy your computer and compromise the information stored on it if the proper anti-virus software were not in place.

Along with antivirus a good firewall must be in place. Firewalls are a huge factor in protecting your computer and network as they provide a theoretical shield that protects your information from those who would like to take a peek and use that information for their own gain. In the case of both firewalls and anti-virus software, it is important to regularly update your protection in order to combat the ever evolving abilities of hackers.

Now that you have your network shielded by a firewall and protected from viruses with your anti-virus program the next step would be to install a good anti-spyware and anti-spam filtering system. Recent studies have shown that over 90 percent of all computers connected to the Internet are infected with spyware. Many spyware programs pop up an official-looking dialog
box asking if you want to download a browser plug-in. These pop-ups may look official, but they are really spyware waiting to install a flurry of pop-ups, undesirable toolbars, or other unwanted content. By installing a good spyware/spam filter the amount of spyware and spam will be drastically reduced, freeing up your valuable resources for more productive use.

Now that we are blocking our network and computers from all these outside threats wouldn’t it be nice to see where the threats are coming from so we can be more proactive instead of reactive to the threats? This leads me into my last recommendation from security and that is an intrusion detection system or IDS for short. An Intrusion Detection System is a defense system, which detects hostile activities in a network. The key is then to detect and possibly prevent activities that may compromise system security, or a hacking attempt in progress including reconnaissance/data collection phases that involve for example, port scans. One key feature of intrusion detection systems is their ability to provide a view of unusual activity and issue alerts notifying administrators and/or block a suspected connection. According to Amoroso [1], intrusion detection is a process of identifying and responding to malicious activity targeted at computing and networking resources”. In addition, IDS tools are capable of distinguishing between insider attacks originating from inside the organization (coming from own employees or customers) and external ones (attacks and the threat posed by hackers).

As information technology professionals not only do we have a duty to protect our networks we also have a duty to protect the students that use our computers and networks. As today’s students become more and more technologically savvy and use the Internet and other technologies for social purposes (sending e-mail, creating Web sites, posting in blogs, sending text messages and images via cell phones, contacting each other through instant messages, chatting in chat rooms and posting to social networking sites), it is not surprising that these technologies are sometimes used to bully other students or harass school staff.

Online bullying, called cyberbullying, happens when teens use the Internet, cell phones, or other devices to send or post text or images intended to hurt or embarrass another person. Some common ways that students are cyberbullied are when other students pretend they are other people online, they will spread lies and rumors about others online, trick people into revealing personal information, send or forward mean text messages or email, and post pictures of victims without consent.

Students can prevent cyberbullying by never sharing their password with anybody else, refusing to pass along cyberbullying messages, tell friends to stop cyberbullying, and blocking communication with cyberbullies. Educators have the right and obligation to supervise and monitor students’ use of the district’s technological resources, and should be on the lookout for improper use of the system to “cyberbully.” Students who misuse the system should be subject to loss of their computer privileges and other forms of discipline as appropriate.
Much of this bullying along with other dangers takes place on social networking sites like Facebook, MySpace, Xanga, and others. Students who post personal information on these sites put them at risk to cyberbullying and also online predators. Technology professionals can play a role by providing instruction to students, staff and parents regarding the safe use of social networking sites and other Internet services. Such instruction might include the dangers of posting personal information online, the fact that other users are not always who they say they are and may be online predators, and how to report inappropriate or offensive content or threats.

As an educational technology professional myself I know what all of you out there are thinking in your head, his ideas on security sound great, protecting our children online is also important, now how am I supposed to do all these with the limited IT staff I have. You are correct in your thinking, IT staffing levels in education are severely lacking. As technology has evolved, the number and complexity of computer systems in the typical school has increased substantially. However, information technology staffing levels have not kept pace, forcing IT staff into a reactive mode.

The lack of IT staff is limiting many schools from realizing the full benefits of technology. For example, the majority of school districts do not have enough staff to plan for or implement new technologies or to integrate technology into the classroom. In addition, school IT staff are stretched thin, supporting more computers and end users than their counterparts in the corporate world.

These staffing shortfalls translate into reduced institution and classroom benefits. A recent survey done by Network World reported that two-thirds of school districts don’t have enough staff to plan for new technology, 55% reported that 50-100% of their department’s workload is spent reacting to technical problems, three-quarters do not have enough staff to implement new technologies and 65% do not have enough staff to integrate technology into the classroom.

With workloads like these it is no wonder that schools face challenges in recruiting and retaining IT staff. Many IT professionals in education feel the pay scale is too low and not competitive enough with similar positions in other industries. Heavy workload, low pay, and not that much opportunity for advancement are probably the biggest obstacles facing IT staff along with funding.

The National Center for Education Statistics reported that school/district leaders view IT as important, but funding issues remain a problem. 49% of those surveyed said the school board understands the importance of IT as it relates to the overall goals but is not as supportive of it financially; 8% felt that their school board did not feel IT was important to the overall goals. One-third felt that their IT budget was severely less than they needed in order to meet the overall expectations of the school board/district. IT funding was identified as the most important issue that needs to be resolved for strategic success.
IT leaders continue to face tight budgets and big expectations. As budgets tighten the approaches to funding IT need to evolve. It is no-longer practical to just depend on one source to fund your IT budget.

To date most school districts take full advantage of federal and state technology funding programs like E-rate. The program provides discounts to assist most schools and libraries in the United States (and U.S. territories) to obtain affordable telecommunications and Internet access. It is one of four support programs funded through a Universal Service fee charged to companies that provide interstate and/or international telecommunications services. My recommendation is for every institute to take advantage of E-rate, the discounts from E-Rate range from 20% to 90% depending on the household income level of the students in the community.

As I mentioned early it is no longer acceptable to rely on one source of funding, E-rate is great and very helpful but you must start to think outside the box and look for new funding sources. Grants, outsourcing services such as email, web hosting, etc. all can provide a big savings to your IT budget. E-school news has a whole section every month on Grants & Funding; they provide links to many different companies that have grants specifically for educational institutes. They also provide grant writing tips on how to get started.

Another option to funding is to get hooked up to one of the numerous organizations that have made it their mission to improve the educational, social and economic opportunities for disadvantaged students and their families by providing them with computers and technology skills for little to no cost. There are free software packages out there that can save schools hundreds of thousands of dollars in software costs. Please refer to my handout for a link to my website which has a list of many companies that participate in these free programs.

The importance of keeping up funding for IT is immeasurable as it relates to the overall goals and mission of the organization. It is up to you as an IT leader to share the vision, the excitement, the advantages that technology brings to our young students to help them compete in the technological world we will set them free in.

Information technology professionals in the K-12 education sector are in a difficult situation. The staffing levels in these departments are low in relation to the number of end users and IT assets they support. Comparisons to IT ratios in non-education industries show that school tech support staff is responsible for about five times as many end users. Staffing shortfalls translate into reduced benefits in both operations and the classroom. The IT workload is primarily reactive, making it challenging for IT leaders to plan for or implement new technologies or to integrate technology into instruction. On top of that you are expected to protect the networks security and patrol students behavior while online. And although school/district leaders are often supportive of IT, and understand its importance to the institution’s overall goals, funding is not always a priority or available.
Even with these challenges, K-12 schools have made some technological advancement. Almost all schools now have an enterprise-level anti-virus solution in place. For the first time funding has fallen out of the top stop as the number one issue facing schools, indicating that some school leaders are starting to see the need to keep funding up. There are many new management/administrative applications on the market that will allow IT staff to manage technology more effectively, freeing up their time for other things. So although as technology professionals we face many challenges ahead, we also face many opportunities.