East Carolina University

Developing and Implementing Technology Security Policies in K-12 Education

Larry Jackson Jr

ICTN 6823

Dr. Phil Lunsford

Summer 2015

Abstract

Because technology is becoming more and more integral to the education community every day, technology managers need to ensure they have well defined policies in place to assist in maintaining the technology that their users depend on. In this paper I will examine the currently accepted principals for implementing Information Security policies in a K-12 educational environment. I will attempt to show an efficient and effective approach that details what steps and considerations should be taken when deciding policies and procedures. Finally I will attempt to convey the importance of a sound security policy and the possible impact of poorly designed and executed policies in an educational environment.

Why are security policies important in educational use?

Technology has become a necessity as a teaching aid in today's modern school systems. With continued growth of the use of technology in our schools administrators have to ensure they have solid policies and procedures in place to maintain the systems needed to further the education of their student population. Because each school system is different in the way they will utilize technology there is no standard as to how to develop or implement policy. Security in itself is a huge concern but understanding how to combat security issues while maintaining a particular environment for your users will make that concern even larger. Users need access to the data you provide and access to the internet to understand it, but where do you compromise on access and security? According to Wells Fargo "Educational institutions are quickly rising to the top of the list of industry segments at risk of a data breach". Today, educational institutions are at crossroads when deciding on what level of security is correct for their environment. In January of 2014 a Texas school district was the victim of a data breach when a thief stole a hard drive and laptop from a school administrator's vehicle. The laptop itself was secured and password protected but the external hard drive was not. Even though the data on the drive was encrypted the thief still had access to the encrypted data. What policies were in place or should have been that could have prevented this? Should administrators be allowed to transport student data away from school grounds? These questions along with hundreds of others will be asked when deciding policies and procedures. Security in educational institutions go far beyond physical security and confidentiality. At this level security has to be an integrated process that is seamless yet understood by all.

Where do you start?

The practice of developing a security policy is a tedious job because you have to protect information as well as your assets but you also have to allow your clients access to that information. Firstly, you need to form a committee or development team that will decide on what will be accepted for the policies and what will be omitted. The team needs to consist of information security technicians, information security managers, WAN/LAN managers, principals and teachers. The group should focus on the usage needs of the student and faculty to determine what policies should be utilized. The life cycle of the development should follow a basic guideline and be conducted in a manner similar to the following phases: initiation, design, implementation, operation/maintenance and replacement. During the initiation phase your team should define the scope and goals of security management within the school district. The goal should be precise yet flexible since technology is always evolving. During this phase you will generate the basic idea of what your internal systems will look like. You will need to conduct technology and feasibility assessments to determine what you have to work with and what if any problems you can or can't prevent. A major drawback seen in education is the fact that at the school level there is a lack of incentive to manage technology efficiently, a lack of sustained funding and technical expertise; but effective policies can help offset if not remedy this (Caspary et al.).

During the next phase, design, it may be a good idea for the security manager or CISO to refer to an established security model instead of trying to recreate the wheel. "Security models provide frameworks for ensuring that all areas of security are addressed; organizations can adopt a framework to meet their own InfoSec need" (Whitman 61). The framework you use will determine the best practices that will be used throughout the district so it must be adapted to fit your schools and the equipment you have. During your design phase you will need to look at the type of devices you will have on your networks and determine the ways they will be secured. You will also need to determine what user devices will be authorized and at what level, what access will be available for adult versus student users, as well as what limitations will be put on web traffic. All assets should be identified and documented with their importance so in the future decisions can be made on what is or isn't an acceptable risk for that asset. For instance, local area networks, how much of a risk will we be taking by allowing data to travel unrestricted vs restricted over it? The idea here is to get a good baseline on your inventory so you can make an educated risk assessment.

The types policies developed in the design phase will fall into one of three categories, governance, technical or procedural. The governance policies will seek to define and describe what your security concepts are and why they are important to your school district (Canavan). Because these policies will be read by technical security personnel and end users, they need to be easily understood by all and clearly state your districts stand on your districts overall security strategy. For example, an annual security awareness program that is administered through the districts website that specifies what is or isn't acceptable use. This program can serve as a formal way of ensuring all employees are up to date on policies since they are considered live documents and are ever changing. The technical policies will be used by your security personnel while they monitor and carry out their duties on a daily basis. These types of policies will be more detailed in nature and cover specific items and how they are to be secured. Good examples of technical policies would be a policy detailing what is needed to secure the AS-400 servers or a policy explaining how users should be authenticated on the wireless network. The technical policies need to be specific in their goals but don't need to have step-by-step guidelines on how to accomplish that goal. When developing these policies ensure that the steps used are kept current to alleviate any confusion when trying to secure an asset. Again, just like governance, technical polices need to be considered live documents. Finally, procedural polices should be put in place to give step-by-step direction on how to carry out a technical policy. These policy types will be used by those in charge of maintaining the assets but don't have to be written by the policy team. It may be more effective for individual departments to write these as they will have more direct experience with the assets. An example of a procedural policy would be the steps needed to physically secure the data center in a school after school hours. This type of policy should be followed exactly until changes to the policy are officially made. A procedural policy will lessen the event of an accidental security breech in your district when followed. The goal again for this phase is to get all of your hardware and software protected by rules or allowances, this in turn will help to ensure risk is minimized and that any security incidents are effectively responded to. Rather than go overboard with countless policies it may be more effective to come up with a shorter list of rules that are easily applies to multiple situations. Just remember "policies that are neither implementable nor enforceable are useless--ten security regulations that are implemented are more effective than 110 that are ignored" (Szuba).

The next phase you will be faced with is implementation of your designed security policies. During this phase you will need to establish a method of deploying your policies throughout your district without affecting the day-to-day operations of your schools. You will need to have an efficient means of disseminating your policies. In general, public websites are a good tool to consider. Using a public website or intranet will give all users easily obtainable access to any policies you implement and are easily updateable when policies are changed. To ensure all users see the policies enacting a means of tracking compliance may be necessary.

Firstly, you would need to have an empowered individual at the school level to be responsible for the accountability of ensuring users at that location are in compliance. One way of achieving compliance is by having users sign digitally sign a form stating that they have viewed and understand the policy is an effective way to track compliance. Staff training may be necessary in some instances, to give users more specialized understanding of the security principles you have enacted. “Reluctance on the part of the organization to adequately prepare staff for making security policy a part of the work environment makes the rest of the effort an exercise in the theoretical--and theory won't protect a system from threats that are all too real” (Sczuba, 32). The goal here is to get to a point where the users aren’t one of the threats that you have to respond to. You will need to communicate to all staff at every level the importance of the new security policies and their importance in assuring they work effectively. All staff members should be required to sign a security agreement before continuing or gaining access to any system after changes are made to policies. Again, by doing so, it ensures that all employees acknowledge the fact that they have read and understand the policy, which may aid you in the future when breaches are found. You want your employees to embrace the new policies not reject or fear them. Explaining to them why the policies were put into place may help some users get over the fear associated with the new guidelines.

During the operation/maintenance phase your system should be up and running and being fine-tuned by your security administrators. Any changes that are found to increase productivity or reduced risk should be made now and the policies should reflect these updates. It would be beneficial for your school level security administrators to conduct another technology assessment to determine what, if any, technology that isn’t covered by the districts technology security plan should be added. Since your policies have been in place for a while only minor adjustments should need to be made, unless totally new equipment or software is being introduced. Monitoring of the systems performance should be an ongoing task to reduce the chances of breaches. End user training should still be accomplished throughout this phase as new staff will continue to enter and exit your district. Keeping your staff up to date on policy changes and refreshment of unchanged policies is still important.

Finally you have reached the end of life for your policies but all this means is that your current policies no longer satisfy your current environment. Not satisfying your current environment can mean anything from not being a feasible option for the hardware/software you currently use or no longer being efficient as a means of deterring threats or breaches. It is time to think about replacing or redefining your policies. This doesn't have to be a full on redo, it can be a refresh of your current guidelines. Since this information is still critical to your district any refinement or replacement should be carefully thought out and evaluated before attempting to replace the current policies. Performing a risk assessment again like you did earlier in the initiation phase will help you determine where your shortcoming are. The key to redoing your outdated policies is data. You need to have the data in place to extrapolate a feasible direction as well as justification for any changes you need to make. The data you take should come from the monitoring of your systems at individual schools and at the district as a whole. The objective of this phase is to get your district back to a point where breaches caused by negligence are at a minimum or even non-existent.

Impact of poorly designed policies.

Sometimes having a poorly designed security policy in place can be as detrimental as having no policy at all. According to Kevin Townsend at ComputerWeekly.com, "…security isn't an application - it's a process. And it is only when it is considered as such and handled as such that we can get close to achieving it”. His comment stems from the fact that users in general seem to think of security as being a program or piece of software to be utilized when in fact it is a way of thinking. If your users don’t think securely then any policies you’ve enacted will be useless in combatting breaches. If a user doesn’t understand a policy because of its wording or because it’s too complicated to comply with then you will ultimately have a huge risk. Your policies need to be clear and easily understandable by all that will be held responsible for them to ensure compliance. By having a poor policy design or no policy at all you leave your district open to any type of breach that finds your vulnerability and not only is your network at risk but all of your data and the data of anyone connected to your network. With more and more districts integrating technology into every facet of the way they educate the need for properly formed policies increases. Long gone are the days where instructors just have to worry about notes being passed in class or verbal rumors making their way around school, in the digital age information flows extremely fast. According to a 2013 study conducted by Pew Research Center, nearly 80% of students between the ages of 12 and 17 have cell phones or similar devises while attending school. These devices should be subject to the same policies as all other technology that is allowed in the school. “Whether in grade school, high school, or college, our children’s learning environment should be safe and secure, and their personal information should remain personal. But digital information and networks bring new dimensions to the threats and risks you grew up with...” (Stewart). A lack of protective polices can and will leave your district open to a myriad of ethical and legal problems. Problems that stem from poor policies can include but are not limited to: computer fraud, abuse, privacy concerns, unauthorized web publishing, copyright infringement, cyber bullying, theft, etc. All these issues can ultimately be lessened if not avoided all together by going through the process of properly planning and implementing good information security policies.

Conclusion

As we all know, technology will continue to become more integrated into everything we do in today's modern world. With this integration into our education systems we will need to ensure that we protect our users and our data. By producing effective and strategic policies we will not only limit, but possibly avoid all together, the number of security incidents occurring by negligence. Although you will never be able to combat every outside threat we may face in an educational system we will at least have procedures in place to effectively deal with them. According to ISO/IEC 27000:2009 the definition of Information Security is the preservation of confidentiality, integrity and availability of information. Without good policies you cannot ensure the confidentiality or integrity of the data you store and use in your districts as there will be no means in place to dictate what methods are used to so. Availability of your data will always be an issue since you don't have procedures in place to deal with problems quickly when they occur. It is not only beneficial for a school district to have good policies it is now required for daily operations to take place and not hinder the teaching of our youth. Effective policies from the

<u>References</u>

Al-Ibrahim, Mohamed H. "Are Our Educational Technology Systems Secure?" International Journal of Innovation, Management and Technology 3.3. Print.

Awad, Hussain, and Fadi Battah. "Are Our Educational Technology Systems Secure?" International Journal of Innovation, Management and Technology 8.5 (2011): 354-58. Print.

Canavan, Sorcha. "Information Security Policy - A Development Guide for Large and Small Companies." SANS Institute InfoSec Reading Room. Web.

Caspary, Kyra. Managing Technology Efficiently in California K-12 Schools: Policies & Practices for Minimizing the Total Cost of Ownership (TCO). Berkeley, Calif.: [Richard & Rhoda Goldman School of Public Policy, U of California], 1999. Print.

Chen, Yan, K. Ramamurthy, and Kuang-Wei Wen. "Organizations' Information Security Policy Compliance: Stick or Carrot Approach?" Journal of Management Information Systems (2012): 157-88. Print.

"K-12 Educational Institutions at Risk: Network Security and Privacy Liability. “June 2015.

http://www.mrt.com/top_stories/article_9935c7a0-8ce3-11e3-b284-0019bb2963f4.html

Madden, Mary, Amanda Lenhart, Maeve Duggan, Sandra Cortesi, and Urs Gasser. "Teens and Technology 2013." Pew Research Center Internet Science Tech RSS. 12 Mar. 2013. Web. 20 July 2015.

Sidhu, Hardeep. "FUNDAMENTAL ISSUES FOR DEVELOPING INFORMATION SECURITY POLICIES." International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) (2012): 99-104. Print.

Stewart, John. "School Information Security." Web. 20 July 2015. http://www.cisco.com/web/strategy/docs/education/School_info_SecurityETL.pdf

Szuba, Tom. "Safeguarding Your Technology: Practical Guidelines for Electronic Education Information Security." National Center for Education Statistics. Web. 15 July 2015.

Townsend, Kevin. "Is Poor Security Worse than No Security at All?" Computer Weekly. Web. 18 July 2015.

Whitman, Michael E., and Herbert J. Mattord. Management of Information Security. Fourth ed. Print.