# Three Reasons for Improving Cybersecurity Instruction and Practice in Schools

Christopher D. Coleman
Academic Services, Computing Center
Louisiana Tech University
Ruston, Louisiana, United States
ccoleman@latech.edu

Department of Learning Technologies
University of North Texas
Denton, Texas, United States

**Abstract:** Information security, or cybersecurity, has become a critical field for modern society. While they may not seem it, schools are a critical battleground for these cybersecurity issues. On the business side, schools maintain sensitive records about students and parents that would be a treasure trove for identity thieves. In their classrooms, high-speed Internet connections and the adoption of 1-to-1 computing and the Internet of Things make school networks an appealing target for hackers looking to build botnets. Meanwhile, the instruction provided is expected to prepare all students with the necessary skills to be productive in a cyber-centric society and encourage a few of them to become the cyber guardians of tomorrow. This paper is a thought-piece intended to raise educator awareness of cybersecurity issues by exploring the world of cybersecurity and providing three reasons why schools should take cybersecurity issues seriously in their administration and their classrooms.

The field of Information Security and Assurance, often referred to more exotically as "cybersecurity," is the field of "securing cyberspace… against abuse, intrusion, and other dangers" (Klaper & Hovy, 2014, p.79). The term cyberspace, as it applies to the digital realm, was coined in fiction by William Gibson – first in his short story *Burning Chrome* (1986) and then more prominently in his novel *Neuromancer* (1988), where cyberspace is defined as "a consensual hallucination experienced daily by billions of legitimate operators, in every nation… a graphic representation of data abstracted from the banks of every computer… [with] unthinkable complexity… [and] clusters and constellations of data" (p. 51). Though Gibson's cyberspace, a name he chose because it seemed like a good buzzword (Neal, Paine, & Pellington, 2000), is more akin to the virtual world popularized in the film, *The Matrix* (Silver, Wachowski, & Wachowski, 1999), the term stuck. Today, though there are many different definitions for cyberspace (Kramer, 2009), the bulk of those definitions tend to define it as relating to the communication networks through which data is transferred and retrieved by people. Most generically, it is used as a synonym for the Internet.

Regardless of its origin, the term is certainly appropriate for what the Internet has become. The word cyber is derived from the word cybernetics, with a Greek root "Kubernetes" meaning "helmsman" (Francois, 1999), that refers to the study of and knowledge related to systems of control. If we accept even the generic definition for cyberspace as being a synonym for the Internet, then it is relatively trivial to observe the control cyberspace exerts over global affairs. When computer networks break down, society can grind to a halt: retail stores stop sales, air traffic stops moving, and even individuals prevented from conducting even the most basic of business now conducted online. Such dependency is easily weaponized, and leads to news stories, such as the Stuxnet attack of 2011 on the Iranian nuclear program, theft of F-35 "Joint Strike Fighter" design data, and campaigns of misinformation during the United States of America's 2016 Presidential election, with major consequences. Cyberspace may be an abstract realm of communication, but its capacity for control and to exert influence on our world and its reality is very real.

Schools are not exempt from this controlling hold of cyberspace. While schools have long been a natural environment for computer use, their presence increased dramatically in the late 1990s with investment in telecommunications infrastructure and computer technology associated with the rapid, universal growth of technology at the time. The declining cost of computers in the 2000s further accelerated this adoption, and would continue to do so as schools pushed towards 1-to-1 computing. Meanwhile, more school functions moved online. Thanks to the advent of the cloud and software as a service (SaaS) subscription models, data systems that would have once required an entire information technology department became available to even the smallest of schools. As a result, administrative tasks once conducted with pencil and paper moved to Web-based information systems, and many classroom tasks have moved online into learning management systems. Technology, arguably brought about a major paradigm shift in schools.

Of course, schools were not the only ones caught up in this shift. While technology was transforming schools, it was transforming society at the same time. Within a span of ten years, wireless internet and smartphones went from cutting edge technologies to commonplace. During that same time, in what seems like the blink of an eye, banking, medical records, property records, tax records, employment records – all moved either from pen and paper or closed electronic systems to Internet services.

The growth is not stopping either. Though the exact number of devices connected to the Internet is a matter of debate, what is agreed upon is that there are billions of them now and there will be tens-of-billions by 2020 (Evans, 2011; Gartner says 4.9 billion connected "things" will be in use in 2015, 2014). This number includes all of the personal computers, laptops, and smartphones we all own, but continues explosive growth due largely to the advent of the Internet of Things (IoT), a vast web of smart devices interacting with one another via the Internet (Evans, 2011). Proponents of IoT promise a more efficient future with better inter-device connectivity, resource management, and even cost savings (Buiocchi, 2017). Individuals are embracing IoT with web-connected appliances, smart televisions, smart home devices, digital assistants like the popular Amazon Echo, and now connected automobiles. Organizations are adopting IoT with smart building controls and network security cameras, and some cities are using IoT to improve city management.

Like other organizations, schools are contributing to this trend as well. On the one hand, schools are adopting many of the IoT approaches also being used in other government agencies and business, such as network cameras, smart climate controls, and other building sensors to improve situational awareness on their campus and improve resource management. On the other hand, teachers are helping to drive IoT as well by embracing things such as wearable technology in the classroom, 1-to-1 learning, data-gathering sensors, computer-based active learning, and other networked learning technologies.

Unfortunately, nearly every pro has its con, and this rapid growth of Internet connected devices certainly has its share of cons. The general threat posed by IoT devices is noted in the cybersecurity field. In early 2014, reports circulated about a cyberattack that had been traced to a smart refrigerator ("Cyberattack traced to hacked refrigerator," 2014). Though there was disagreement as to whether the refrigerator was really to blame ("Despite the news, your refrigerator is not yet sending spam," 2014), there is consensus that the IoT is the next frontier in cyber-crime. This is sobering news considering the finding by an HP research team that at least 60% of IoT devices contained at least one type of serious vulnerability (Hewlett Packard Enterprise, 2015). IoT vulnerabilities have since led the U.S. Federal Bureau of Investigation to issue strong warnings concerning consumer use of IoT devices ("Cyber tip: Be vigilant with your Internet of Things devices", 2015). Though IoT devices have promise in shaping the classroom of the future, each of these devices brings a very real cybersecurity risk to the classroom.

This increase in risk comes against a seemingly contradictory backdrop of less-than-effective cybersecurity practices in schools coupled with an awareness of its importance in instruction. A research study commissioned by the National Cyber Security Alliance indicated that 99% of technology coordinators, 97% of administrators, and 91% of teachers surveyed believed that cybersecurity should be taught in schools (2011). 62% of those responding also felt that cybersecurity was an important aspect of professional development (National Cyber Security Alliance, 2011). While 81% of administrators and 67% of teachers claiming to be prepared to discuss cybersecurity with students, 50% of teachers indicated not having taught anything related to cybersecurity within a 12-month period (National Cyber Security Alliance, 2011). 23% of teachers covered the cybersecurity principle of strong passwords, making it the most popular principle taught (National Cyber Security Alliance, 2011). Yet, despite a clear indication that both conventional and emerging security threats will increase (PricewaterhouseCoopers, 2014), education still

lags behind other industrial sectors in cybersecurity. Security firm Bitsight ranks education a distant last in information security effectiveness (2015).

On the face of it, these findings tend to indicate a disconnect between attitudes and practice with respect to cybersecurity instruction in schools. If over 91% of teachers surveyed think cybersecurity is important and over 67% feel comfortable discussing it in class, then one might expect more than 23% to discuss something as fundamental to cybersecurity as password strength. Granted, there were limitations in this study due to a seemingly broad variety of teachers surveyed. One would not expect, for example, English teachers to provide instruction in cybersecurity as much as a computer literacy teacher. If anything, these shortcomings illustrate that cybersecurity instruction at the K-12 level is neither consistent, suggesting that cybersecurity standards may be an order, nor is it fully understood. This is unfortunate, as promoting cybersecurity at the K-12 level is both an important element in fostering basic digital citizenship in students (Ribble, 2015) and in preparing students with skills needed to alleviate the current shortage of workers with cybersecurity expertise (ISC2, 2017).

It is difficult to say exactly why cybersecurity practice and instruction is in its current state in education. Perhaps it is because cybersecurity is an emerging need to which schools have been slow to adapt? Perhaps it because teachers do not believe they have the skills necessary to address cybersecurity issues in the classroom? Another possibility, is that cybersecurity is often conceived of as a business function. That is, cybersecurity is more of a concern of policymakers and information technology managers than it is of teachers and other school administrators. Unfortunately, there does not appear to be a great deal of literature on the subject of educators' attitudes towards information security, as others have noted (Younes, 2013).

While such research gaps in our understanding of cybersecurity in education are desperately in need of closing, that does not change the fact that the issue grows worse with time. The cybersecurity talent shortage will not fix itself, and education does not occur in a vacuum insulating it from changes in technology. On the contrary, education often embraces new technology to further enhance instruction. Unfortunately, that technology can bring with it new security threats to schools and to the educational process. It is imperative that an attempt be made to understand and mitigate these threats and to help solve the cybersecurity problems society now faces. Thus, I would like to propose three reasons why schools should take cybersecurity issues seriously.

## Reason One: The Ethical Argument

It is fitting to begin with the ethical argument, because ethics form the foundation of almost all human decisions and activity. Consider, that a common feature of professional groups is the creation and adherence to a code of ethics (Bersoff, 1995). From attorneys to psychologists and doctors to engineers, the majority of professional societies appear to have some stated code of ethics. These ethical codes are developed to ensure that members practicing a given profession do so with a consistent ethical framework. This is true of educators as well. The National Education Association (NEA) and American Association of University Professors (AAUP) have codified ethics. In learning technologies specifically, the International Society for Technology in Education (ISTE) and Association for Educational Communications and Technology (AECT) have codified their own ethical standards.

Unfortunately, the review of literature thus far does not indicate that an ethical argument for strengthening information security in schools has been broadly articulated; however, the notion of an ethical duty to protect the privacy and information of other people underlies the entire cybersecurity field. Whether protecting assets, data, or privacy, there is an underlying ethical decision-making process that drives the way in which we respond (or not) to cybersecurity issues. Moreover, the traditional juxtaposition of cybersecurity professionals as the "white hat" protectors against malicious "black hat" hackers implies that ethical values, and not skills or technology, serve as the greatest dividing line in the cybersecurity world.

Perhaps the greatest ethical directive in any field is that which derives from medicine's Hippocratic oath and its derivations: to avoid causing harm or injury. While this notion is certainly applicable to the field of cybersecurity itself, it is a documented idea in educational technology literature. Spector (2016) contends that ethics are an "essential aspect of educational technology" (p.1003). To this end he (2005; 2016) proposed the idea of an "Educratic oath." Spector (2016) admits that the oath has not caught on, and has since moved his focus towards a general treatment of values. Nevertheless, the preeminent concern of doing no harm remains throughout.

If we, as educators, have an ethical obligation to do no harm to our students, then we surely have some ethical obligation to protect our students from harm. The wide scope of such an obligation is suggested in laws that require teachers and other school officials to report suspected child abuse to authorities (Crosson-Tower, 2003). This scope expands even further when educators are tasked with reporting or intervening with bullying and cyberbullying ("Key components in state anti-bullying laws," 2014), all while maintaining compliance with privacy laws. It stands to reason then, that if we have an ethical responsibility to protect students from physical violence and predators, both on- and off-line, then we have an ethical responsibility to protect students from other threats online as well.

An important point that should be made in our treatment of ethics is that ethics are just as much about the controls and limitation we place on our own behavior to protect students as it is about protecting them from external threats. Consider, for example, the Pennsylvania class-action lawsuit *Robbins v. Lower Merion School District*. In this case, the school district sought to secure devices by installing software that would allow district personnel to access built-in webcams to capture evidence in the event the computers were stolen (2010). Given the computers were intended for a 1-to-1 environment and that students would be taking the computers home, the potential for privacy invasion should have been considered by the district and appropriate policies made and notification given to users. The district instead failed to provide any notice to students or their parents of this functionality, and further failed to make adequate policy governing the circumstances in which this functionality might be enabled. The result, after this technology was discovered following a student being disciplined based on a photo taken by the computer in the student's bedroom, was a class-action lawsuit and a subsequent $610,000 settlement (Martin, 2010) that underscores the need for schools to consider both their ethical obligations as well the need appropriate technology governance policies and processes to ensure those ethical obligations are enforced.

Exactly what these obligations look like in practice is not an easy question to answer, and it has some overlap with the arguments that are to follow. For now, it should suffice to say that we have demonstrated that educators accept some sense of responsibility for protecting their students. To this end, we as educators, should also have a similar compulsion to accept some responsibility for the protecting our students from cyber threats. At the very least, this should mean giving them the resources to protect themselves and committing ourselves to practices that consider the cyber threats to our students.

## Reason Two: The Business Argument

The business case is the traditional and most common rationale for cybersecurity in almost every environment. This rationale for cybersecurity focuses on the organization's operational context, and seeks to limit damage to the ability of the organization to function effectively. This means taking steps to ensure the confidentiality, integrity, and availability of the data that the organization needs to function. This can often focus on things such as physical device security to guard against theft, network security, and continuity of operations or disaster recovery planning to help ensure that organizational operations minimally affected by and are quickly restored following any incident.

It is tempting for many, when thinking of cybersecurity from a business case perspective in schools, to believe that school data is of little value outside of the school. On the contrary, despite typically not being organized to seek profit; schools manipulate a great deal of valuable data. Even in K-12, schools store information on students and their parents that can include social security numbers, e-mail addresses, credit card numbers, financial data, and other personally identifiable information (PII) that could be stolen and sold on the black market. While an individual record may not be of great value, the economies of scale make such information valuable on the black market where just e-mail addresses can be sold in blocks of 1,000 for anywhere from $10 to $200 ("Prices of computer hackers and online fraud").

Student PII is not the only information of value educational institutions may have. Independent schools and school districts may have human resource departments that maintain databases of sensitive information on their employees as well. Additionally, they likely have business offices that, at least, manage accounts payable that provide access to organizational financial data. In the case of private schools or colleges, they may also process accounts receivable, including student tuition payments, that provides access to student financial information. Research universities in particular are vulnerable due to their ownership and management patentable research and development (Rothwell, Lobo, Strumsky, & Muro, 2013). Theft or preliminary release of such information,

especially on proprietary or controlled designs, could, at minimum, cause irreparable financial damage to a university.

A major part of the business case for cybersecurity is ensuring the integrity of the core business processes that drive the organization's value. For schools, this value largely rests in their ability to assess student performance and provide appropriate matriculation credit. After all, students ultimately attend school with the expectation of some form of completion – moving to another grade or completing a diploma or degree. As a result, assessment is a cornerstone of the educational process, and its integrity is critical to the business of education. Bialazewski, makes an excellent observation related to the business case for cybersecurity in schools, suggesting that assessment data is in need of better protection (2015). He notes a number of incidents where students may be tempted to cheat, and have been caught engaging in computer crime in order to facilitate such cheating. This assessment data, which goes beyond just student test scores, can include experimental test banks, current test banks, or other information that could seriously compromise testing processes and undermine the assessment process.

It is also worth considering that exfiltration or manipulation of data may not be a hacker's objective. According to a U.S. Department of Education report, 99% of public elementary and secondary schools in the United States had some form of Internet access by 2001 (U.S. Department of Education, 2002). According to the same report, 84% of those Internet connections are of types that are generally considered to be "high speed" and "always on" (U.S. Department of Education, 2002). A large number of computers attached to a persistent network connection make schools a tempting target for hackers looking to establishing a botnet, or a network of computers they can use to launch attacks on other targets. The malware required to establish such a network can open computers to additional vulnerabilities, slow network connections, and can cause other disruptions to computing services that can disrupt instruction.

In other cases, a hacker's objective may be less clandestine. Barth (2017) writes of an incident where pro-ISIS hackers redirected the webpages of 800 schools, all using the same webhost, across the United States to a website displaying an ISIS recruitment video. Meanwhile, the U.S. Department of Education (Rodrigue, 2017) has issued several warnings about attackers targeting schools who may steal student, parent, and faculty information, and then use that information extort the school into paying a ransom or by threatening the individuals directly. News reports indicate that these threats are not theoretical or imaginary. Rios (2017) reports that schools in at least three states have been targeted by attackers who have held school data for ransom or who have threatened physical violence. In the best of situations, these are threats that are require investigation. Depending on their severity, these incidents can disrupt instruction briefly or bring the instructional business of the institution to a halt. In either case, such incidents significantly interfere with an institution's ability to fulfill its instructional mission.

School leaders and administrators should not be under any illusions about their status as a target. Being proactive about cybersecurity can help schools reduce their chance of being adversely affected by malicious activity, and can help to ensure that the core educational functions of the school are able to proceed without interruption due to cybersecurity incidents.

## Reason Three: The Instructional Argument

The third, and final, argument for enhancing cybersecurity in education lies in instruction. To be clear, this argument has nothing to do with preventing cyber incidents from interfering with instruction itself (since that is a component of the business argument just made), but it is, instead, the idea that cybersecurity should be factored into the decisions we make about the things we teach and in way in which we teach them.

Dewey (1934) suggested that the chief function of education was to provide our young with the things they needed to systematically progress into members of our society and that, as a result, education is a product of sociological context. Education, therefore, ultimately serves the needs of the society that educates. While the exact needs are a matter of debate in the literature, there are two themes that emerge: education is to help individuals develop into productive citizens and to acquire skills that are relevant to the workforce (Adler, 1982; deMarrais & LeCompte, 1995; Tyack, 1988).

In his discussion of the social context of education and the skills needed for an increasingly technical world, Dewey (1934) spoke of the progression of technology and its influence on the subjects added to students'

courses of study. Since Dewey's time, technology has marched on far beyond railroads, telephones, and automobiles. Just as those technologies changed instruction in Dewey's time, and before, so new technologies demand changes in our instruction now. Computers changed instruction in the past with the introduction of computer science and information technology education, and though they have been around for some time now, the ever-expanding use of computers continues to add to the educational needs of society.

The ubiquity of computers and the rise of digital society has, like the technologies before, changed the skills individuals need to function in society. Current thinking is that schools must participate in building and teaching the norms associated with a digital society (Ribble, 2015) – this, in a nutshell, is digital citizenship. Among the many concerns related to building digital citizenship, Ribble lists cybersecurity as a major component of instilling digital citizenship. Just as we teach students how to become functional members of society in other ways, so we must also teach them how to function and work in digital society. Part of knowing how to live and work in a digital society is having the skills necessary to protect digital information. Schools should take the lead in ensuring that students are adequately prepared with the basic skills necessary to protect themselves from threats lurking in cyberspace, as well as have the cybersecurity literacy needed to be employable in the modern workforce.

Digital citizenship and basic cybersecurity skills and literacy are not, however, the only issues schools are positioned to address. Recall, from the beginning of this paper, the discussion of the current state of the cybersecurity skills shortage (ISC2, 2017). While universities are certainly expected, as a stop-gap, to train people for today; K-12 schools are educating the cybersecurity professionals of tomorrow. If we accept both that cybersecurity is a critical need for modern, digital society and that schools are, in some way, responsible for raising up students who can address society's needs, then is necessary, that K-12 schools take steps to ensure that they are offering skills and opportunities to cultivate future cybersecurity talent.

Teaching these skills to students means that we must have some teachers who are both capable and willing to speak to cybersecurity issues in their classes. This presents schools with the opportunity to meet multiple needs through training. Cybersecurity awareness training is used in many organizations to influence employee behaviors and encourage more secure behavior (McCrohan, Engel, & Harvey, 2010). Well-designed professional development opportunities can meet the need of schools to provide information security training while simultaneously giving them the content-knowledge and self-efficacy required to engage students in the classroom regarding cybersecurity issues. One would expect that this would be desirable, given that 62% of teachers were reported to believe that cybersecurity training was a high priority in their career development needs (National Cyber Security Alliance, 2011).

Trained teachers will be better positioned to bring cybersecurity principles into the classroom. Better trained teachers will be able to more effectively mentor students with respect to cybersecurity principles, meeting the need of students to learn about the prevalence of cybersecurity threats, ways in which they can protect themselves from such threats, and thus providing them more robust skills for digital citizenship and future employment.

## Conclusion

There can be little doubt that the practice of cybersecurity is here to stay. As it has grown more critical for other industries, so it has grown and will continue to become a critical area in education. Schools must do a better job in protecting students and teachers from cyberthreats, both conventional ones as well as the threats that could emerge from the advent of the Internet of Things. Further, schools must come to see cybersecurity as more than an operational exercise or a subject to be taught, and come to regard cybersecurity as an ethical issue that requires balance. We must balance the needs of organizational security with the privacy needs and rights of students and teachers, and be prepared to use ethical principles to make sound decisions regarding the application of technology. Schools must regard information security issues as not simply business decisions, but as ethical decisions. Educators have a responsibility to protect students and prepare them to be good digital citizens and the digital guardians of tomorrow.

## References


Adler, M. J. (1982). *The Paidea proposal: An educational manifesto*. New York: Collier Macmillan.

Barth, B. (2017, November 7). Hundreds of school websites redirected pro-ISIS web page. *SC Magazine*. Retrieved from https://www.scmagazine.com/hundreds-of-school-websites-redirected-pro-isis-web-page/article/705985/

Bauman, V. (2015, September 17). Hackers breach Commack High School computer system, district officials say. *Newsday*. Retrieved from: http://www.newsday.com/long-island/education/hackers-breach-commack-high-school-computer-system-district-officials-say-1.10857943

Bialaszewski, D. (2015). Information security in education: Are we continually improving? *Issues in Informing Science and Information Technology*, *12*, 45-54. Retrieved from http://iisit.org/Vol12/IISITv12p045-054Bialaszewski1770.pdf

BitSight Technologies (2015). *Third annual BitSight insights industry benchmark report*. Retrieved from http://cdn2.hubspot.net/hubfs/277648/Insights/Q315_BitSight_Insights_Energy_Utilities.pdf

Bersoff, D. (1995). *Ethical conflicts in psychology* (3rd ed.). Washington, D.C.: American Psychological Association.

Buiocchi, T. (2007, December 5). Driving operational cost savings with the Internet of Things. *MIT Sloan Management* Review. Retrieved from https://sloanreview.mit.edu/article/driving-operational-cost-savings-with-the-internet-of-things/

Crosson-Tower, C. (2003). *The role of educators in preventing and responding to child abuse and neglect.* Retrieved from U.S. Department of Health and Human Services website: https://www.childwelfare.gov/pubPDFs/educator.pdf

Cyber tip: Be vigilant with your Internet of Things devices (2015, October). *FBI News Blog*. Retrieved from https://www.fbi.gov/news/news_blog/cyber-tip-be-vigilant-with-your-internet-of-things-iot-devices

Cyberattack traced to hacked refrigerator. (2014, January 17). Retrieved from http://phys.org/news/2014-01-cyberattack-hacked-refrigerator.html

deMarrais, K. B., & LeCompte, M. D. (1995). *The way schools work: A sociological analysis of education (2nd ed.)*. White Plains, NY: Longman Publishers.

Dewey, J. (1934). Individual psychology and education. *The Philosopher.* Retrieved from http://www.the-philosopher.co.uk/2016/08/individual-psychology-and-education-1934.html

Evans, D. (2011). *The Internet of Things: How the next evolution of the internet is changing everything.* Retrieved from http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Francois, C. (1999). Systemics and cybernetics in a historical perspective. *Systems Research and Behavioral Science*, 16(1), 203–219. doi: 10.1002/(SICI)1099-1743(199905/06)16:3<203::AID-SRES210>3.0.CO;2-1

Gartner says 4.9 billion connected "things" will be in use in 2015. (2014, November 11). Retrieved from http://www.gartner.com/newsroom/id/2905717

Gibson, W. (1986). *Burning Chrome*. New York: Arbor House

Gibson, W. (1988). *Neuromancer.* New York: Berkley Publishing Group

Hewlett Packard Enterprise. (2015) *Internet of things research study.* Retrieved from http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en

ISC2. (2017). *2017 Global information security workforce study: Benchmarking workforce capacity and response to cyber risk*. Retrieved from https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf

Key components in state anti-bullying laws. (2014). Retrieved from https://www.stopbullying.gov/laws/key-components/index.html

Kramer, F. D. (2009). Cyberpower and national security: Policy recommendations for a strategic framework. In F.D. Kramer, S.H. Starr, & L.K. Wentz (Eds.) *Cyberpower and National Security*. Retrieved from http://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-01.pdf

Martin, J. P. (2010, October 12). Lower Merion district's laptop saga ends with $610,000 settlement. *Philadelphia Inquirer*. Retrieved from: http://articles.philly.com/2010-10-12/news/24981536_1_laptop-students-district-several-million-dollars

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal of Internet Commerce*, *9*(1), 23–41. doi: 10.1080/15332861.2010.487415

National Cyber Security Alliance (2011). *The state of K-12 cyberethics, cybersafety, and cybersecurity curriculum in the United States*. Retrieved from: http://www.staysafeonline.org/download/datasets/2052/2011_national_k12_study.pdf

Neale, M., Paine, C., & Pellington, M. (Producers), & Neale, M. (Director). (2000). *No Maps for These Territories* [Motion picture]. United States: Docurama.

Prices of computer hackers and online fraud. (2015). *Havocscope global black market information*. Retrieved from: http://www.havocscope.com/black-market-prices/hackers/

PricewaterhouseCoopers (2014). *US cybercrime: Rising risks, reduced readiness*. Retrieved from: https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf

Ribble, M. (2015). *Digital citizenship in schools* (3rd ed.) Washington, DC: International Society for Technology in Education.

Rios, E. (2017, October 25). Hackers are stealing sensitive student data – And schools are paying thousands of dollars to get it back. *Mother Jones*. Retrieved from http://www.motherjones.com/crime-justice/2017/10/hackers-are-stealing-sensitive-student-data-and-schools-are-paying-thousands-of-dollars-to-get-it-back/

Robbins v. Lower Merion School District, No. 10-665 (2010).

Rodrigue, T. (2017, October 16). ALERT! – CyberAdvisory – New Type of Cyber Extortion/Threat [Electronic mailing list message]. Retrieved from https://ifap.ed.gov/eannouncements/101617ALERTCyberAdvisoryNewTypeCyberExtortionThreat.html

Rothwell, J., Lobo, J., Strumsky, D., & Muro M. (2013) *Patenting prosperity: Invention and economic performance in the United States and its metropolitan areas.* Retrieved from Brookings Institution website: http://www.brookings.edu/~/media/research/files/reports/2013/02/patenting-prosperity-rothwell/patenting-prosperity-rothwell.pdf

Silver, J. (Producer), & Wachowski, A. & Wachowski, L. (Directors). (1999). *The Matrix* [Motion picture]. United States: Warner Brothers.

Spector, J. M. (2005). Innovations in instructional technology: An introduction to this volume. In J.M. Spector, C. Ohrazda, A. Van Schaack, & D. A. Wiley (Eds.), *Innovations in instructional technology: Essays in honor of M. David Merrill* (pp. xxxi-xxxvi). Mahwah: Erlbaum.

Spector, J. M. (2016). Ethics in educational technology: towards a framework for ethical decision making in and for the discipline. *Educational Technology Research & Development, 64*(1), 1003–1011. doi: 10.1007/s11423-016-9483-0

Thomas, P. (2014, January 23) Despite the news, your refrigerator is not yet sending spam. *Symantec Official Blog*. Retrieved from http://www.symantec.com/connect/blogs/despite-news-your-refrigerator-not-yet-sending-spam

Tyack, D. B. (1988). Ways of seeing: An essay on the history of compulsory schooling. In R. M. Jaeger (Ed.), *Complementary methods for research in education (pp. 24-59)*. Washington, DC: American Educational Research Association.

U.S. Department of Education, National Center for Education Statistics, Office of Educational Research and Improvement. (2002). *Internet access in U.S. public schools and classrooms: 1994-2001* (NECS Publication No. 2002-018). Retrieved from National Center for Education Statistics: http://nces.ed.gov/pubs2002/2002018.pdf

Younes, W. (2013). *Cybersecurity education (training and awareness) for K-12 faculty and staff in Allegheny county* (Order No. 3577772). Available from ProQuest Dissertations & Theses Global. (1490983194). Retrieved from http://search.proquest.com/docview/1490983194?accountid=7113