Journal of Cybersecurity Education, Research and Practice

Volume 2024 | Number 1 Article 3

October 2023

Leading K-12 Community Responsiveness to Cyber Threats via Education of School Community

Michele Kielty
James Madison University, kieltyml@jmu.edu

A. Renee Staton
James Madison University, statonar@jmu.edu

Recommended Citation

Kielty, Michele and Staton, A. Renee (2023) "Leading K-12 Community Responsiveness to Cyber Threats via Education of School Community," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2024: No. 1, Article 3.
DOI: https://doi.org/10.32727/8.2023.28
Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2024/iss1/3

Leading K-12 Community Responsiveness to Cyber Threats via Education of School Community

Abstract

Cyber threats have escalated in recent years. Many of these threats have been direct and vicious attacks on K-12 systems. Educators are rarely trained on how to address cyber threats from a systemic and educational perspective when such challenges arise in their school buildings. This article explains the cyber threats that are looming large for K-12 systems and provides concrete tools for school leaders to employ in order to provide preventive education to their school communities.

Keywords

cyber threat, K-12, school community, K-12 cyber, cyber intelligence

Cover Page Footnote

We acknowledge Dr. Edna Reid, Founder of the James Madison University's Cyber Intelligence Graduate Certificate Program, for her mentorship and encouragement,.

Leading K-12 Community Responsiveness to Cyber Threats via Education of School Community

Michele L. Kielty
Department of Graduate Psychology
James Madison University
Harrisonburg, VA, USA
kieltyml@jmu.edu
https://orcid.org/0000-0001-7956-4332

A. Renee Staton
Department of Graduate Psychology
James Madison University
Harrisonburg, VA, USA
statonar@jmu.edu
https://orcid.org/0000-0003-3693-6073

***Abstract*— Cyber threats have escalated in recent years. Many of these threats have been direct and vicious attacks on K-12 systems. Educators are rarely trained on how to address cyber threats from a systemic and educational perspective when such challenges arise in their school buildings. This article explains the cyber threats that are looming large for K-12 systems and provides concrete tools for school leaders to employ in order to provide preventive education to their school communities.**

Keywords— cyber threat, K-12, school community, K-12 cyber, cyber intelligence

I. SCHOOLS AS CONTEXT

K-12 is a term used in the United States to indicate the number of years publicly supported in primary and secondary education [13]. According to [6] there are there over 130,000 schools in the United States. K-12 environments, often divided into elementary, middle and high schools are susceptible to a number of internal and external cyber threats.

Internally, a vast amount of information is held within computerized systems in K-12 education. Examples of internal information about students include place of residence, standardized test scores, academic and learning disability testing, mental health records and other permanent files such as grades and discipline reports. Parental details linked to students include details such as place of residence, income, and court documents such as custody orders. Parents also may have credit card and bank information on file for automated payments for things like school meals. Examples of internal information about staff includes employment records, salary information, comments made on student records, and multiple communications like emails to other staff members and administrators. Threat actors might access information internally via shoulder surfing, dumpster diving, and stealing important documents on site [25].

Externally, there are many potential cyber threats. Individual schools interface with many computing systems that contain vital records, school records, financial information about students and families, and personnel information about employees (including evaluations and salary and other financial information). Examples of these systems are Powerschool [22] which is an online grading and record keeping as well as notes tracking behavioral and mental health concerns; and College Board [5] and Naviance [6] which are systems that interact with institutions higher education to share test scores and sensitive college application materials. State education agencies' online networks collect computerized standardized test scores of K-12 students. External threats include external hackers finding their way into systems to gain and spread information about students, families, and staff. These attacks can happen via phishing, social engineering, ransomware, and hacktivist activities aimed at school reform.

II. SCHOOLS AND CYBERSECURITY

Threat actors have been expanding theft efforts and cyber attacks on K-12 school communities across the nation [4] Examples of possible external cyber threats in school communities are phishing, social engineering, ransomware, shoulder surfing, dumpster diving, pretexting and many other threats such malware in the form of worms, and Trojan horse viruses [27]. Out of all of these threats, ransomware has emerged as one of the most significant.

School employees and students are frequent victims of cyber crimes. Solutions need to be understood and disseminated by school leadership in order to mitigate the negative effects of these crimes. Reference [19] aptly noted, "Cybersecurity education and skills training is an unavoidable endeavor for all federal, state, and private organizations… The authors believe that such training should start in K-12…" Cyber intelligence is a term that indicates understanding cyber threat issues as well as relevant prevention and mitigation strategies.

Cyber intelligence includes tracking, analyzing, and countering security digital threats**.** The steps of cyber intelligence include planning, collection, analysis, production, dissemination and feedback [18]. According to [12] cyber intelligence is defined as "the products and processes across the intelligence cycle of assessing the capabilities, intentions, and activities – technical and otherwise – of potential adversaries and competitors in the cyber domain (with cyber counterintelligence as a sub-discipline)" (p.2). Cyber intelligence efforts are need to counteract adversaries' efforts, which continue to proliferate especially with the unfolding of the COVD-19 global pandemic crisis. According to the Department of Homeland Security [7] malicious actors are taking advantage of the crisis by engaging in scams through phishing, malware distribution, registering related domain names, and attacking new teleworking and remote access infrastructure.

Cyber intelligence is relevant to K-12 education for many broad reasons. First, several authors have noted that there is a significant lack of awareness and training of professionals as well as students in the area of K-12 education and cyber intelligence [3, 19, 31]. In addition to educating adults in K-12 buildings, it is important to increase students' access to information, training, and hands-on experience, through experiences like competitions and simulations, with cybersecurity [3, 24, 31]. It is noteworthy that there is a need to improve access to cybersecurity awareness, training, and practice for underrepresented populations [24] Through cyber intelligence efforts, cybersecurity can be better ensured for K-12 school systems.

A. Sensitive data and cyber threats specific to schools

School systems are vulnerable to cyber threats because they contain a vast amount of sensitive data in computerized systems. According to [13],

> Educational institutions possess social security numbers, medical records, financial data, and intellectual property of faculty, staff, and students, making them lucrative targets. Add that cybersecurity preparedness is among the last among industry segments for K-12 schools and post-secondary schools, it makes full sense why cybercriminals are targeting them.

Ransomware, as well as phishing proliferated throughout the COVID-19 pandemic. Recent reliance on online platform has increased the vulnerability of most school systems. The Department of Homeland Security [7] cautioned, "attackers have been able to hijack teleconferences and online classrooms that have been set up without security controls (e.g., passwords) or with unpatched versions of the communications platform software".

How common are cyber threats to K-12 institutions and what are the consequences of these threats? Reference [4] noted that the cyber-security firm Armor found ransomware infections at 54 educational organizations, such as like school districts and colleges, at over 500 locations. Reference [16] reported the Department of Education found that more than 60% of schools targeted by hackers in 2016-2017 choose to pay a ransom to reclaim their data. Also, according to the FBI Cyber Division [11], multiple attacks targeted at schools were carried out by a group called TDO, which stands for TheDarkOverlord (TDO). TDO was responsible for at least 69 intrusions into K-12 schools and other businesses. While it is difficult to determine how likely it is for each individual school system to be targeted by cyber criminals. It is clear that consequences of these ever growing attacks can be detrimental, both financially and operationally to school systems.

III. Relevant Protective Measures for K-12 Schools

Cybersecurity efforts are taking place on both national and local levels in order to protect students, employees, and families. Significant legislation has been introduced to protect K-12 school communities. The Homeland Security and Government Affairs website [7] explains that the *K-12 Cybersecurity Act of 2019* ensured that Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) will work with other government and private organizations to complete a study of cybersecurity risks to K-12 systems. Sensitive student and employee data will be better protected as a result and the CISA will be tasked to create online toolkit to help schools improve cybersecurity.

According to the Readiness and Emergency Management for Schools (REMS), when a cybersecurity incident occurs, the team should consider reporting the incident to one or more of the following legal agencies: the FBI (via the Field Office Cyber Task Force); the Internet Crime Complaint Center, the National Cyber Investigative Joint Task Force;the National CybersecurityandCommunicationsIntegrationCenter;or the US Computer Emergency Readiness Team [25].

To help protect children and to ensure their privacy, safety, and confidentiality online, several laws apply [25] . First, the Family Educational Rights and Privacy Act (FERPA) gives parents and student the right to review and inspect educational records, and to file a complaint if records are compromised. Second, the Children'sInternetProtectionAct (CIPA) helps protect children from obscene or harmfulcontentontheInternet. This law states that schools or libraries that receive discounts through Universal Service Program for Schools and Libraries, mut prove that they have an Internet safety policy that blocks or filters inappropriate or harmful content such as obscene or pornographic materials. Finally, the Protection of Pupil Rights Amendment (PPRA) applies to schools and contractors that receive Department of Education funding. Parents have the right to preview instructional materials and must approve of survey, analyses, or evaluation that reveal certain information about students and families [53].

Specific prevention measures can be implemented in K-12 buildings, possibly by a Central Office cyber security team or system IT personnel. A technical report suggests a variety of strategies to address multiple layers of security [9]. Specifically, six defensive security techniques that can be very useful in schools include: firewalls, software patch management, anti-malware protection, back-up and recovery, two-factor authentication, and web proxy server. According to [9], **firewalls** provide additional levels of defense that support the traditional routers, and they create more rules for network segments or zones to communicate to each other. **Software patches are critical** because software programs are susceptible to attack and can be vulnerable to hackers as they are looking for weak spots (i.e. outdated or weak programs). **Anti-malware protection** analyzes emails for threats such as zero-day exploits that come through in malicious attachments. This protection, often in the form of anti-malware software, can protect organizations against phishing, ransomware, and other attacks.

Back-up and recovery, especially via cloud services, can be critical to K-12 cyber functioning. Cyber attacks typically impact machines, but not cloud back-ups. According to [28], using cloud services can be cost effective. **Two-factor (or multi-factor) authentication** allows access only after presenting two or more pieces of evidence. This can be very useful for teachers, parents and students who are looking to access web-hosted school resources that hold sensitive information, such as PowerSchool. Finally, **proxy servers** often act as firewalls and web filter as they serve as intermediaries between end users and website they are browsing. Traffic flows through the proxy server in both directions, forwarding requested and received data. The layer or protection is important in K-12 schools when so many people are browsing the web for multiple reasons.

A. Basic solutions to common cyber threats

As cyber threats continue to increase for K-12 systems, it is important to have a basic set of guidelines for students, staff, and families in order to reduce the number and seriousness of data breaches. It is also important to have both prevention and intervention strategies to handle cyber threats, First, basic cyber hygiene is preventative Figure 1 includes suggested do's and don'ts that are accessible for all school-based constituents. The suggestions are specific and easy to follow.

B. Application of the disaster management cycle in K-12 systems

Table 1. Cybersecurity awareness handout for school-based constituents

DO's	DON'TS
DO Institute a culture of security awareness: Instill a culture of responsible information and stewardship and insist that cyber security be taken seriously	**DON'T Be the user error:** Use good security software
DO Manage your own devices: Update regularly, password protect, and reinforce with students	**DON'T Be a rogue clicker:** Never click on e-mail attachments unless you know the sender
DO Store sensitive information: Use secure servers with encryption; only use protected laptops	**DON'T Be caught by the "Phishers":** Phishing occurs when a bad actor sends out emails or texts that pretend to be from a trusted source such as the IRS or your bank
DO Maintain good password habits: Keep them secret, refresh on a schedule, don't use for multiple applications, and consider using vault software	**DON'T Be pick-pocketed:** Never click on an email asking you to verify financial or personal information
DO Closely monitor school-related and personal credit cards and bank accounts: Banks do not catch everything, so be sure to monitor	**DON'T Click on short cuts:** Be wary of using "dark web" file-sharing software through which illegal copies of software, music, or movies are shared
DO Manage your own privacy: Pause to consider how much information you reveal, no system is immune from hacks, including security systems	**X Be behind the times or forget to back it up:** Enable automatic updates and back up your personal and professional data, which can be held for ransom or lost
Source: [2]	**Source: [15]**

In addition to the guidelines offered in Table 1, ways to defend against online attacks related to online learning can be shared with students, staff, and families in writing, via short presentation or video trainings accompanied by short quizzes. Due to the recent increased usage of online meeting platforms, the Federal Bureau of Investigation [10,11] published guidelines for avoiding such attacks. These tips include requiring a meeting password and creating a waiting room for guests, not sharing meeting links on social media where they can easily be accessed, minimizing screensharing options (i.e. only allow host to screenshare), making sure the updated version of the meeting applications are being used (i.e. the version with the most fixed bugs), and enduring that clear policies exist and are distributed with regard to information and physical security.

IV. Responding to Security Breaches Systemically

Internally, a vast amount of information is held within computerized systems in K-12 education. Externally, there are many potential cyber threats. The network security is variable among school systems. Lack of resources and lack of training K-12 constituents (staff, students, and families) is a well-documented problem, as is the increase in ransomware threats for K-12 schools. In order to address issues and problems with cybersecurity in K-12 education, implementing strong recovery plans once a threat has occurred, is another very important function.

While protective measures can be implemented proactively, schools mut be ready to respond if a breach occurs. In this section, various methods for responding to cyber threats are reviewed using three approaches: one includes general prevention strategies [17], another includes the NIST framework [21], and the third is an application of a disaster management cycle [20, 31].

Related to a general overall approach [23] noted, in the *Threat Intelligence Handbook*, that there is a typical incident response process. This process includes incident detection (via alert), discovery about how the incident has happened, triage and containment to mitigate the threat, remediation to repair damages and remove infections, and passing the incident to "business as usual" teams to finalize actions. Reference [17] also offered a general incident response approach that seems relevant for K-12 systems. It starts with assembling the Incident Response Team (IRT), which would be made up of an Information Security Officer (ISO), technical leads, human resources, public relations, risk management, and business matter specialists.

After assembling the IRT, [17] recommend following these steps: 1. Determine authority to call an incident; 2. Assign IRT responsibilities; 3. Do not assign severity levels; 4. Establish communications procedures and responsibilities; 5. Gather pertinent information; 6. Outline the process and 7. Review and test the plan. These steps, along with an example of a K-12 incident response, are shown in Figure 2. In the K-12 example shown in Figure 2, there are seven steps, each having one to three corresponding actions.

Step 1: Determine authority to call in an incident	**Step 2:** Assign IRT Respon-sibilities	**Step 3:** Do not assign severity levels	**Step 4:** Establish communication procedures and responsibilities	**Step 5:** Gather pertinent information	**Step 6:** Outline the process	**Step 7:** Review and test the plan
Action A: Alert principal	**Action A:** Teacher or student alerts principal	**Action A:** All incidents are considered top priority unless proven otherwise	**Action A:** Meet in Central Office "war room" if significant threat	**Action A:** Consult list of IRT members to make are all are alerted	**Action A:** Record escalation points	**Action A:** Review plan quarterly
Action B: Alert Central Office IT who can declare incident	**Action B:** Principal alerts Central Office IT		**Action B:** IRT consults with law enforcement to determine course of action	**Action B:** Communica te with all vendors whose programs are involved	**Action B:** Record steps taken	**Action B:** Update list of IRT members
	Action C: IT decides whether or not to alert law enforcement		**Action C:** Superintendent determines how to communicate with families after briefed by IRT		**Action C:** Create list of lessons learned	**Action C:** Schedule annual practice to test plan

Figure 1. Incident response example of K-12 cyber attack

A. *NIST framework*

The National Institute of Standards and Technology (NIST) provides a NIST Cybersecurity framework. The NIST Framework includes the steps of: **Identify, Protect, Detect, Respond, and Recover** [21] In order to prepare a K-12 community to prevent cyber threats, one must first identify the major needs of the school and also their areas of vulnerability. A protection strategy includes designing a training geared towards education staff and students to help prevent the threats, including information noted in Figure 1. The detection process would be helping K-12 communities recognize red flags and suspicious activities and to respond appropriately, asking for help when needed. The school would also need a protocol for responding to and recovering from a threat if it did occur (i.e. someone clicked on a suspicious link and ransomware was installed). An example of this protocol is show in Figure 2. Reference [26] puts mitigation at the center of the NIST framework and uses it as a prevention strategy.

B. *Application of the disaster management cycle in K-12 systems*

Reference [1] noted,

> School districts collect gobs of data, much of which is required by law. Every state has laws about data retention. For schools and districts, losing data without the means to recover it is a major issue. And schools are easy targets for cyberattacks because of persistent struggles with resources, particularly IT staffing and funds. Unfortunately, many schools lack recovery plans. Reference [1] recommended modeling recovery on a disaster recovery model.

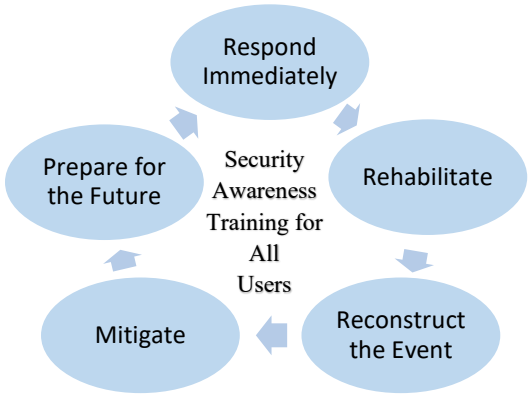

Figure 2. Recovery for cyber security in K-12 settings via disaster management

Using a Disaster Management Cycle (DMC), modeled on [18] as well as advice from various authors on how to implement a recovery plan in K-12 education, the lead author created the model depicted in Figure 2. The DMC incorporates steps of **Respond**, **Rehabilitate**, **Reconstruct**, **Mitigate**, **and Prepare for the Future**, which are illustrated in Figure 2. Because users are the biggest threat in K-12 settings, due to lack of training and awareness as well as low incidence reporting (and propensity to click on phishing emails) the most important aspect of a recovery plan is working to educate users about best practices [1]. Reference [29] gave specific to-do's for school systems. The following paragraph illustrates specific action items for each step.

In the **Respond** step, schools should immediately follow school monitoring, detection, and reporting protocols. They should proactively respond by implementing a layered security approach including things like firewall, antivirus protection, patch management, and strict controls on software admin and install. For the **Rehabilitate** step, schools should have more than one reliable backup method for records in place, restore functions and resume services as soon as possible. For the **Reconstruct** step, schools should collect all evidence of the root cause of the incident, document every action taken, and create and track recovery metrics to understand the nature and dimensions of the attack. The **Mitigate** phase should put protective measures in place to protect future losses (i.e. require updated and more complex passwords and restrict admin access to very few individuals. Finally, in the **Prepare for the Future** phase, schools should: test and evaluate recovery efforts; practice and perfect techniques; and finally, evaluate technology, security awareness training content and backup records [29].

In examining Figure 2, it should be noted that the central core is "Security Awareness Training for All Users" which includes staff, students, parents, and other personnel. This is because of the seriousness of cyber threats issue in K-12 education, and the reality of lack of resources to hire more cyber intelligence and IT professionals, requires that users be as equipped as possible to help spot and win battles against cyber threat actors (CTA's). The **Respond** step is at the top of the diagram and refers to the need to immediately follow school monitoring, detection, and reporting protocols. Reference [4] noted that part of being proactive includes implementing a layered security approach (i.e. firewall, antivirus protection, malware protection, patch management, and strict controls on software installation and admin privileges).

The **Rehabilitate** function refers to having more than one reliable back up location for records (i.e cloud-based that are easy to recover—not only Gsuite). The **Reconstruct** step involves collecting all evidence of the root cause of the incident. Reference [4] highlighted the importance of document actions, as well as gathering data in the form of metrics related to technical details of the attacks. The **Mitigate** step refers to putting protective measures, such as requiring frequent password updates and restricting admin access to a small number or professionals, in order to prevent future losses. Finally, the **Prepare for Future** step involves testing and evaluating recovery efforts. Evaluating technology (making sure it is up to date), reviewing security awareness training content, and analyzing current back-up methods to make sure they are aligned with current best practices are all important.

V. Conclusion and Recommendations

In conclusion, countless cyber attacks have taken place in K-12 school settings. These attacks are creating problems for school systems, which are often under-resourced in terms of finances and personnel. The prevalence of school-based cyber attacks is not a question of "if" they will happen, rather a question of "when" [17]. Shoring up a strong cyber intelligence teams to prevent and respond to threats is critical. School constituents must be trained on best practices for cyber threat protection and prevention. Properly skilled personnel are not a "nice to have," rather, they are a "need to have." Cyber threats for K-12 schools are expected to increase, therefore, we must be responsive to these needs.

Schools have become a much more vulnerable target in recent years, especially in the area of ransomware [4, 15]. School constituents, including students, staff, and families should be protected from cyber criminal activity. In order for this protection to be available, many more resources are needed for funding IT and analyst positions, as well as for providing adequate training for staff and students. Layered systems of protection must be put into place for cybersecurity efforts to be adequate and worthwhile. Additionally, plans for responding to cyber threats should be clear and the personnel responsible for responding every step of the way needs to be evident to everyone. Recovery efforts can be more effective if good back-up and security is in place and if the team is well-resourced in terms of time and talent to respond actively and proactively. In summary, the authors recommend hiring and training cyber intelligence and cyber analyst professionals in K-12 settings as well as empower K-12 community

constituents by training them to spot and help defeat cyber criminals.

In summary, this article provided a current context for cyber threats in K-12 educational settings, Prevention and intervention strategies were explained and models for implementing these strategies were illustrated. Resources for school leaders to prevent and respond to cyber attacks were shared.

References

[1] Andrade, D. (2019, October 30). Hey, IT Leaders: When disaster strikes, will your school be ready?: K–12 districts are targeted for cyberattacks every day, and administrators should have a plan to prevent complete data loss. Retrieved at: https://edtechmagazine.com/k12/article/2019/10/hey-it-leaders-when-disaster-strikes-

[2] Arlitsch, K., & Edelman, A. (2014). Staying safe: Cyber security for people and organizations. *Journal of Library Administration*, *54*(1), 46-56. http://dx.doi.org/10.1080/01930826.2014.893116

[3] Chattopadhyay, A., Christian, D., Ulman, A., & Petty, S. (2018, September). Towards A novel visual privacy themed educational tool for cybersecurity awareness and K-12 outreach. In *Proceedings of the 19th Annual SIG Conference on Information Technology Education* (pp. 159-159). International World Wide Web Conferences Steering Committee.
https://doi.org/10.1145/3241815.3241883

[4] Cimpanu C. (2019, October 1). Over 500 schools. Retrieved at: https://www.zdnet.com/article/over-500-us-schools-were-hit-by-ransomware-in-2019/

[5] College starts here https://www.collegeboard.com

[6] Connecting learning to life https://www.naviance.com

[7] Department of Homeland Security (2020, April 8). Alert (AA20-099A): COVID-19 exploited by malicious cyber actors. Retrieved at: https://www.us-cert.gov/ncas/alerts/aa20-099a

[8] Education statistics: Facts about American schools (2019, January 3). Retrieved at: https://www.edweek.org/ew/issues/education-statistics/index.html

[9] Fabro, M. (2007). *Control systems cyber security: Defense-in-depth strategies* (No. INL/CON- 07-12804). Idaho National Laboratory (INL).

[10] Federal Bureau of Investigation. (2020, March 30). FBI warns of teleconferencing and online classroom hijacking during COVID-19pandemic [Press release]. https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

[11] Federal Bureau of Investigation Cyber Division (2018, January 31). Cyber criminal group threatens schools and students.Retrieved at: https:// www.edtechstrategies.com/wp-content/uploads/2018/02/FBI-CyberCriminalsSchools.pdf

[12] Force, C. I. T. (2015). Cyber intelligence: Preparing today's talent for tomorrow's threats. *Intelligence and National Security Alliance (INSA)*.

[13] Fortinet (2017). Mapping the ransomware landscape: Understanding the scope and sophistication of the threat. Retrieved at: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/WP-Mapping-The-Ransomware-Landscape.pdf

[14] Glavin, Chris (2014-02-06). Education in the United States. K-12 Academics". Retrieved at https://www.k12academics.com

[15] Goldsborough, R. (2016). Protecting yourself from ransomware. *Teacher Librarian*, *43*(4), 70.

[16] Goud, N. (n.d.). K12 schools are vulnerable to ransomware cyber attacks. Retreieved at: https://www.cybersecurity-insiders.com/k12-schools-are-vulnerable-to-ransomware-cyber-attacks/

[17] Hayward, L., & Quinn, M. (2016). It's not if but when: How to build your cyber incident response plan. New York: Kroll.

[18] Intelligence studies: Cyber intelligence (2019, September 7). Retrieved from: https://usnwc.libguides.com/c.php?g=494120&p=3381599.

[19] Javidi, G., & Sheybani, E. (2018). K-12 cybersecurity education, research, and outreach. In *2018 IEEE Frontiers in Education Conference (FIE)* (pp. 1-5). IEEE. https://doi.org/10.1109%2Ffie.2018.8659021

[20] Khan, H., Vasilescu, L. G., & Khan, A. (2008). Disaster management cycle-a theoretical approach. *Journal of Management and Marketing*, *6*(1), 43-50.

[21] Mahn, A. (2013, October 23). Identify, Protect, Detect, Respond and Recover: The NIST Cybersecurity Framework. Retrieved from https://www.nist.gov/blogs/taking-measure/identify-protect-detect-respond-and-recover-nist-cybersecurity-framework

[22] Personalized education for every journey https://www.powerschool.com

[23] Pokorny, Z. (Ed.) (2019). Threat intelligence handbook (2nd ed.) Cyberedge Press: Annapolis.

[24] Pusey, P., Gondree, M., & Peterson, Z. (2016). The outcomes of cybersecurity competitions and implications for underrepresented populations. *IEEE Security & Privacy*, *14*(6), 90-95. https://doi.org/10.1109/msp.2016.119

[25] Readiness and Emergency Management for Schools (REMS). *Cybersecurity considerations for K-12 schools and school districts.* ssRetrieved from: https://rems.ed.gov/docs/Cybersecurity_K-12_Fact_Sheet_508C.PDF https://doi.org/10.1201/b12700-29

[26] Risk Mitigation. (2018). Retrieved from https://www.cyberwatching.eu/risk-mitigation

[27] Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4), 89.
https://doi.org/10.3390/fi11040089

[28] Stern. M (2012, October 10). Cyber intelligence: Identifying the threat and understanding the terrain in cyberspace. Retrieved at: https://www.securityweek.com/cyber-intelligence-identifying-threat-and-understanding-terrain-cyberspace

[29] Todev, N. (2018, January 16). Here's how to develop a cybersecurity recovery plan. Retrieved at: https://www.convergetechmedia.com/heres-how-to-develop-a-cybersecurity-recovery-plan/

[30] Unify your technology: Unlock potential. https://www.powerschool.com

[31] Warfield,C. (n.d.) *The Disaster Management Cycle*. Retrieved from https://www.gdrc.org/uem/disasters/1-dm_cycle.html