An Institutional Risk Reduction Model for Teaching Cybersecurity

Erik Moore, Daniel Likarish, Bobbie Bastian, Michael Brooks

An Institutional Risk Reduction Model for Teaching Cybersecurity

Erik Moore[1[0000-0003-1566-526X]], Daniel Likarish[1[0000-0001-5654-710X]],
Bobbie Bastian[2[0000-0003-4223-8247]]michael brooks[2[0000-0001-9447-7245]]

[1] Regis University, Denver, Colorado 80221, USA
{emoore,dlikaris}@regis.edu
[2] Adams 12 Five Star Schools, Thornton, Colorado 80241 USA
{bobbie.r.bastian,michael.brooks}@adams12.org

Abstract. This work presents a model for reviewing the risks of institutions teaching cybersecurity. The work is based on efforts in this direction at Regis University and Adams 12 Five Star Schools in Colorado. These two institutions are described in a comparative case study reviewing the following four aspects of addressing risk: policy, adjudication, infrastructure protection, and curricular boundaries. The model is presented in a generalizable framework to facilitate risk analysis across the education of children in public schools, university level education, and professional development programs. This framework is not intended to supplement a traditional threat analysis program and not replace it. In addition to the specialized risks addressed here, institutions teaching cybersecurity are often perceived as potential targets for adversaries because of the schools as a pipeline to cyber defense activities, and because institutions teaching cybersecurity are part of societal long-term cyber defense strategies that confront criminal, nation state, and activist threats

Keywords: Cybersecurity, Cybersecurity Curriculum, Cybersecurity Education, Ethical Policy, Policy, Adjudication, Infrastructure, Risk Management, Risk Mitigation, Cyber Defense, University Cybersecurity Program, K-12 Cyber Security, Threat Analysis, Risk Framework

1 Introduction

Cyber risk for an institution that teaches cybersecurity goes beyond baseline cybersecurity and includes behavioral risks that develop as student populations acquire and practice newfound cybersecurity skills. The study presented here covers two cases, a public school district where cybersecurity skills are taught to minors, and a university where cybersecurity is taught at the undergraduate, graduate, and professional development levels. This study reviews risk mitigation efforts across a broad range of education activities from extra-curricular risks with students starting at about 13 years old to the training of long-time cybersecurity professionals embedded in the industry. A multi-layered risk mitigation framework is used to methodically present the cases.

The sense of urgency that drove the formulation of this paper comes from many stories that the authors have heard over the last few years from peers at other cybersecurity programs. A school's curricular WordPress websites end up hacked shortly after a cybersecurity teacher reviews the exploits with students. A cybersecurity competition encourages minors to actively practice red team activities without that competition organization addressing the inherent risks institutions face in developing those skills in students whose executive functions may not be mature enough to handle the habituated behavior. And minors are occasionally convicted of crimes after learning exploits in a high school environment. [1]

While teachers and institutions may fall back on, "but we had them sign an ethical agreement" the authors see this as falling short of the full range of institutional responsibilities inherent in reducing the risks of teaching cybersecurity. These risks are not only to the institution, but to the parent, the student and the communities in which they hope to thrive. This paper provides an initial set of materials to open up greater discourse in this area, spurring questions like, "What should the limits be on curricular and extracurricular content for various groups of students?", "Can cybersecurity curricular content analysis spur coordinated work in the institution's risk mitigation strategy?" The work of Marquardson and Garmillion [2] presents clear description of risk and control categories in this area, acknowledging and addressing the risks of institutions teaching cybersecurity. In contrast, the work presented here analyzes two cases spanning the public education of children, through university level activities, and to ongoing professional development in cybersecurity, addressing each level. The cases presented describe the practices and formal efforts within the programs of Adams 12 Five Star Schools (Adams 12) and Regis University, both in the State of Colorado, USA.

At Regis, the practices that led to this policy was developed on the Academic Network run by the college faculty and the network's Project Scientist. At Adams 12 the program was spurred by the development of the first cybersecurity course. This paper is part of an effort to expand these initial practices and formulate policy. One challenge that spurred the work forward was the need to evaluate multiple cyber competitions for Kindergarten through 12th grade appropriateness. While education institutions are subject to the same cyber attacks all institutions face, we designed this model to increase awareness in addition to general cybersecurity practice. [3]

2 Research Methodology

The method used in this study is the presentation and comparison of two cases to analyze a range of practice, and develop models that can demonstrate coherence and usability across that range. The cases are presented in parallel structure, reviewing specific areas of risk and identifying variance in both risk and the practice of mitigating risk between the institutions. While some aspirational notes are made, the cases are based on actual institutional practice and efforts at risk mitigation. The risks addressed here are in regards to institutional and personal behavioral outcomes.

The work of Fujs, Mihelič and Vrhovec, suggest that the case study method is one of the more commonly used research methods in cybersecurity analysis [4]. Their observation that achieving credibility through triangulation is applied here in practice, using four lenses of observation across the two cases. In terms of the use of qualitative methods in general, Creswell and Creswell [5] suggest that a focused research question, based on the post-positivist perspective, can drive the analysis of the topic in question.

The analysis of this case attempts to answer the question, are there controls that can be added to social behavior that can assist in the mitigation of risk across a range of institutions teaching cybersecurity? We present two cases where current controls are used across both the public education of children and the adult education towards degrees and professional development. The analysis formulates both common and unique elements of these practices into a model. Analysis of the case attempts to understand whether, from an institutional level, can we form a coherent model that accommodates differentiators while maintaining a coherent framework. Then, we pose the question, could such a model support a risk mitigation strategy that might be applied across a broad range of education and training programs. This research does not collect data about individual learners, but focuses on the institutions, programs, and structures that contain the inherent risk. Data is gathered from the research team's interviews and experiences participating in the cases as members of those institutions.

3 A Layered Risk Mitigation Framework for Analyzing Cyber Education Risks

The four layers of risk mitigation work introduced here in Table 1 specifically address the cybersecurity challenges of institutions that teach or train in cybersecurity disciplines. The layers represent areas where the authors offer case analysis and methods being used at their institutions to mitigate risk. Following that, gap analysis suggests work yet to be done to address risks within the two cases. Then the authors reflect on the generalizability of the work and follow-on research on their roadmap that might support broader efforts to address the particular risks of institutions teaching cybersecurity.

Table 1. The framework for comparing layers of protection for schools teaching cybersecurity to children in public education and to adults at the college and professional level.

Framework Comparing Layers of Protection of Institutions Teaching Cybersecurity	
Adams 12 Five Star Schools	**Regis University**
Limits on teaching risky content areas to minors in curricular and extracurricular contexts	Limits on teaching risky content areas to adult learners and institutional partner members
Technical cybersecurity controls	Technical cybersecurity controls
Ethical training and adjudication with student and parents	Ethical training and adjudication with adult learners and institutions
Ethical policy and agreements with students and parents	Ethical policy and agreements with adult learners and institutions

The framework above was developed through a comparative review process of risk mitigating measures related to cybersecurity programs with the authors, who are the developers of each of these areas within their respective institutions. As individual controls were reviewed in an extended way, the authors extracted the pattern of this layered approach.

The authors chose a framework that spans public education of children and higher education because both institutions in this paper are already spanning that full range. Regis offers outreach programs to children in public and private education. Adams 12 is offering courses for college credit in association with a local college. Career pathways to higher education and articulation with higher education are even required to receive federal funding for computer science courses such as the Perkins grant. [6] The combined framework is designed to facilitate transparent collaboration between different types of institutions. By developing highly generalized structure, each institution has the freedom to evaluate their specific content and cybersecurity posture with local relevance.

Ethical policy and agreements lay the foundation of what is acceptable and unacceptable behavior for students, establishing boundaries for both ethical use of technology and specifically the appropriate use of institutional technology, learned skills, and access to resources and information. Ethical training and adjudication relates more to the curricular goals of helping students understand the personal and professional ethical standards, and intervening with guidance or punitive measures when necessary. Technical network containment is a widely used model for behavioral control in hands-on cybersecurity programs in terms of technical risks that addresses external risks and general student user behavior. As a basic control, network compartmentalization is still very necessary and is based on a strong foundation of policy that has generally been outward-facing towards hackers and the Internet. These controls could apply to students studying a variety of laboratory-based information technology programs and extracurricular activities where some malicious behavior occasionally occurs on institutional systems.

4 A Case of Cybersecurity Coursework, Competitions, and Professional Training for Adults

Adams 12 needed to address three use cases to reduce institutional risk while providing cybersecurity education training infrastructure. Regis serves college students from freshman through graduate programs where autonomous choices and career readiness is required. Regis also provides cybersecurity training that includes technical physical exercises for active cyber defense teams and cyber security professionals. In addition to these core services, Regis offers community outreach workshops of a few hours each to children in public schools.

Regis has delivered these hands-on cybersecurity training resources to support a variety of modalities over the past twenty years. The risk reduction measures presented below were developed during the period when the authors developed expertise in the protecting following:

- Online and classroom delivery of cybersecurity labs using modern network and data centers structures.
- Cybersecurity laboratory environment where development, experimentation, and analysis can take place. Classroom-based learning using user interface, compute cycles, data storage, virtual machines, laptops, etc.
- Cyber range environment for a variety of competitions including the Rocky Mountain Front Range CANVAS exercise and the Rocky Mountain region of the Collegiate Cyber Defense Challenge (RMCCDC).
- Agilely deployable "Cyber Gymnasium" where various challenges and components can be rapidly deployed to meet the training needs of various partners, user groups, etc.

The college-level laboratory instructional design, including coursework associated laboratory assignments and graduate research programs, was developed utilizing Malcom Knowles principles, enriching the adult learner experience [7]. For Regis, class-associated laboratory work and academic research facilities have been closely integrated into the day-to-day functions of the Regis Cyber Range. This network facility sits separate from the production networks of Regis University Network and is primarily controlled by a Project Scientist and the faculty of the College of Computer & Information Sciences.

Groups coming in for training that use ready-made modules from the "Cyber Gymnasium" are provisioned with resources the same way that new classes are brought online. Guest participants included contexts like ISSA, ISACA, and ISC.

Cyber competitions like CANVAS and the RMCCDC require major reconfiguration of the Cyber Range to accommodate large numbers of participant teams, vigorous interactions between computers, and provisioned networks in classrooms dedicated to the particular events. In addition to significant network changes, the Regis staff and faculty must welcome large numbers of students and faculty from other institutions, and a highly diverse range of cybersecurity professionals supporting the event.

Cyber defense training is a more complex capability. When The State of Colorado and National Guard visited a RMCCDC competition and short training exercises performed by Regis for the professional organization ISSA (Information Systems Security Association), they requested that Regis host a cyber defense training event on the Regis campus using the Cyber Range.

Cyber outreach programs generally serve children in public schools starting at about age 13. Regis used several pre-existing extracurricular programs to forward this work either on a Regis campus, or on-site at the schools. The programs used are the nationally recognized CyberPatriot and locally organized Cyber Girls. The goal is for boys and girls in underserved and established middle school and high schools to harden these systems in particular ways that score points based. Students receive a list of vulnerabilities and must mitigate the vulnerabilities locally on the VM to score points.

4.1 Ethical Policy and Agreement

In general, where cybersecurity guidelines extend beyond standard institutional policies, the institution relies on the Association of Computing Machinery [10] and various ethical standards publications within the sector professional organizations such as EC Council.

Upon enrollment, students must agree to the student handbook. The section Responsible Use of University Technology Resources generally covers technology behavior on the Regis network and on the Internet in general. These rules cover the prohibition of unauthorized access, malware distribution, impersonation, exploitation of system vulnerabilities, and misuses of data. The Regis University Catalog covers plagiarism, cheating, and other types of academic integrity issues. Beyond this initial policy, course content covers ethics training, and is described here under the section on adjudication.

The Outreach programs for children with public institutions and for college students at the RMCCDC events, student groups must have a faculty sponsor for guest teams from each institution represented. This is important to adjudicate behavioral issues as students participate at their home institutions, or as a group at Regis. Students inherit their institutions behavioral policies, but Regis considers the maturity of the institutions they are working with. The RMCCDC boundaries of acceptable behavior to maintain the game rules [11] were set for all regions by the National Collegiate Cyber Defense Competition (NCCDC), focusing on defensive practices known as “Blue Team” work rather than attack practices known in the competition as “Red Team” work.

Generally, for joint events like the RMCCDC and training challenges, adjudication can happen within the competition, including things like time limits for performance, prohibition of social engineering other teams, and restrictions from accessing off-site data stores. Of more significant interest is the directives associated with the long-term ethical behaviors the competition is attempting to instill in participant behavior as persistent personal and professional traits. These significantly also address the protection of the game infrastructure, and the institutional infrastructure on which the game

resides. In the RMCCDC specifically, each Blue Team does not counterattack, but follows the rules of engagement that civil institutions must follow in the professional and local government worlds. The Red Team is an active part of the game space provided by the game hosts to provide adaptive attacks as part of the competition.

Professional and cyber defense training depends on the ethical guidelines of the partner institutions and professional organization for reducing risk, as they establish the relevant boundaries of behavior for the activities pertinent to those organizations. This suggests that a professional development workshop for the Information Systems Audit and Control Association would have different boundaries of behavior than a joint cyber defense training exercise with the Colorado National Guard.

4.2 Technical Cybersecurity Controls

The Regis Cyber Range operates under a separate Internet connection. It uses its own firewalls and internal security monitoring, and has its own methods of compartmentalization, assigning clusters of system to various classes using virtualization software. The only link between the Cyber Range and the Regis production network is the federation of accounts that allows for access to be controlled in-part on the affiliation status with Regis University.

The Regis Laboratory Network environment is on the same infrastructure as competition activities. To divide these functions, networks are segmented into separate virtual networks that are adapted to the particular goal. When a cyber competition is hosted, a part of the Cyber Range can be "virtual air-gapped" to emulate a logically independent network. For Regis, this makes deployment much more agile than a physical detachment, and would generally have traffic filtering for security control. This type of containment has been sufficient given the greater separation with the Regis Production Network. The technical controls apply only to the Regis campus, and so behavior at home must rely on the policy and adjudication for reducing risk.

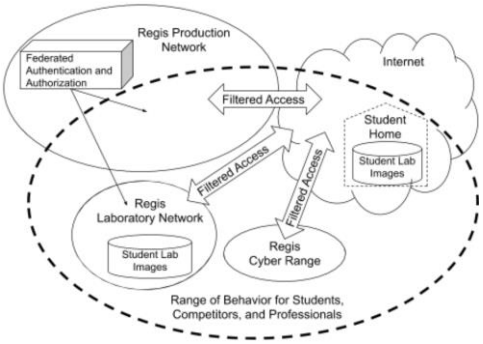

Fig. 1. Range of Encouraged Student, Competitor, or Professional Behavior at Regis University

Outreach programs offered to public school children by Regis University, regardless of whether at the student's local school or on the Regis campus, are offered through stand-alone hardware not connected to a network. Programs like CyberPatriot have specific curriculum to load, and in other cases Regis develops and loads software. This means that the technical controls on risky student behavior and the possibility of disruptive hacks from the Internet are greatly reduced. Therefore, this function is not drawn on the diagram of technical controls, except that the range of student behavior after the event still extends to the Internet and home where Regis must rely more on ethical training to mitigate risk.

4.3 Ethical Training and Adjudication

For Regis students, the adjudication of policy violations for both academic integrity and inappropriate use of technology resources is handled by the Integrity Committee with an appeal to the Academic Integrity Board of the appropriate college. To give students an active understanding of issues related to Students have embedded sections in each course that provides ethical content engaged in the topics appropriate to course content. The process invokes corrective actions is the primary resolution but sanctions and potentially expulsion are possible.

The adjudication of fairness of the competition; the persistent ethics that the RMCCDC is working to instill in participants; and the aspirational skills that the competition is encouraging are all reinforced through practice. These two levels of rules published prior to the event provide students with guidelines that focus their efforts on defending systems.

For professional adjudication, Regis requires that the organizational representative for any particular group respond appropriately to resolve issues and enforce policy. Regis reserves the right to exclude disruptive, unethical, and malicious network or human behavior from its premises. This is handled by the Regis staff hosting an event, and can be escalated through the appropriate college.

4.4 Limits on Teaching Risky Content Areas

Regis University educates and trains a range of student and professional learners looking to engage in the cybersecurity community in both professional cybersecurity and cyber defense roles. But Regis does not allow it's systems to be repurposed for those activities, or produce disruptive effects outside the Regis controlled Cyber Range environments. The Regis production network may not be used as an experimental network for visitor or student exploits or security experiments.

In order to establish and maintain these boundaries of content, demonstration, and laboratory work Regis refers to the general ethical guides for staff and faculty. Specifically, course content is the responsibility of the Regis Program Chair, ensuring that course content is free of high risk activities. Course content that has proactive cybersecurity work such as penetration testing, and malware reverse engineering have ex-

tensive ethical components so that students understand the professional constraints and ethical expectations associated with these activities.

5 A Case of Cybersecurity Education and Extracurricular Programs for Children

Adams 12 Five Star Schools is a public school district north of Denver, Colorado USA serving just under 40,000 children with just under 5,000 staff. Like many districts in the region, Adams 12 is adopting cybersecurity curriculum and extracurricular activities to support both the career potential of graduates and the interest of students. Adams 12 offers several opportunities for students to gain experience, skill, and knowledge in cybersecurity.

The cybersecurity curriculum taught in Adams 12 is based on the Cybersecurity Curriculum Framework published on the National Cryptologic Museum Foundation [9] website. This framework, along with the text: Cyber Security Principles and Practices 4th Edition by Stallings and Brown [12], units from the NICERC Cyber Society curriculum [13], and resources from clark.center [14] make up the instructional materials for the class.

Curricular hands-on opportunities beyond general safety start with an 8th grade course lasting about three months emphasizing privacy, encryption, and decryption. At the high school level, students can take a year-long course in cybersecurity that progresses along the NIST Framework [15], and uses the CIA triad of confidentiality, integrity, and availability [16] of data as a framing perspective when dealing with each topic. While both 8th grade and high school coursework have modules covering ethics, the High school course has a section emphasizing law.

Currently CyberPatriots is the only extracurricular cybersecurity activity offered at Adams 12, available from 6th grade through graduation at 12th grade. This program comes with strict behavioral and ethical guidelines for all participants that the District follows. A particular characteristic of CyberPatriot in relation to other cyber competitions available is that it is focused exclusively on cyber defense and does not involve attack training as other competitions offer offensive security competition, red teaming, or capture the flag competitions [17].

5.1 Ethical Policy and Agreement

Adams 12 employs several policy strategies to ensure that students and parents are aware of the districts behavioral expectations and to create a safe community where the risks of using the Internet are reduced in general. Specific policies and practices are enforced through both teacher oversight, and through the formal policy development process of the Institution. District policy goes through a policy review board and the students and parents sign a technology use agreement that refers to the District policy of acceptable use. Cybersecurity presents specific risks that may not be fully covered by the Adams 12 district policy, so additional controls are implemented as described below.

As cybersecurity classes start, the teachers communicate during the first two weeks of school, students receive the class syllabus. The syllabus lays out the units and skills taught in the course, and class expectations. The syllabus has a page that is required to be signed by students and parents. The page that is signed by students and parents collects current parent contact information, preferred method of contact, information about if parents want a code to be able to monitor the work students complete and submit in Schoology, and information about the ways parents can be involved in the classroom and school community. This includes being a guest speaker, volunteering, sitting on the district CS Advisory Committee, or helping with co-curricular events.

In regards to extracurricular policy, Adams 12 and the CyberPatriot organization require teams to register. Once teams are registered, students sign-up for one of the teams via online access If a parent does not complete the verification, and the student competes in the competitions, the team score will be withheld until parents have signed off on allowing their student to participate. In January of each year, Adams 12 hosts an open house. During the open house parents and potential students learn about all of the computer science programs available at Adams 12 including cybersecurity. Families are given an overview of what is taught in each class. In April of each year, Adams 12 hosts Pre-Acceptance night. During Pre-Acceptance Night parents and students come and learn about the specifics for each class. A presentation is given on the specific curriculum in the class. If a student is interested in taking the class once they have heard more about it, they fill out an application that evening. The counselors check to see that each student has met the prerequisites for the class, has appropriate grades and attendance to be successful in the class. This spring we will be introducing the parent cybersecurity course agreement during pre-acceptance. Both parents and students will sign the agreement when applying for the course. Similar to the Advance Placement (AP) contract that parents and students sign when applying for AP computer science. At the end of August, students register for CyberPatriot and form teams and parent approval is required. In October, Adams 12 hosts parent-teacher conferences. Both parents and students attend the conferences. During the conferences, parents have the opportunity to ask any questions that they currently have. Parents are shown the curriculum and resources that students have access to including Schoology, Co-Curricular calendars, and Plural Sight. Parents have the opportunity to get a parent code for Schoology to monitor their student's assignments and work.

5.2 Technical Cybersecurity Controls

Adams 12 runs a production network to perform the operations of the business and schools, using various forms of network segmentation including Virtual LANs and access control lists between them that isolate where the traffic from varying systems to what is required. Figure 2 illustrates the range of network types available within Adams 12 including the Production Network, Cyber Competition Network, and Air Gap Network.

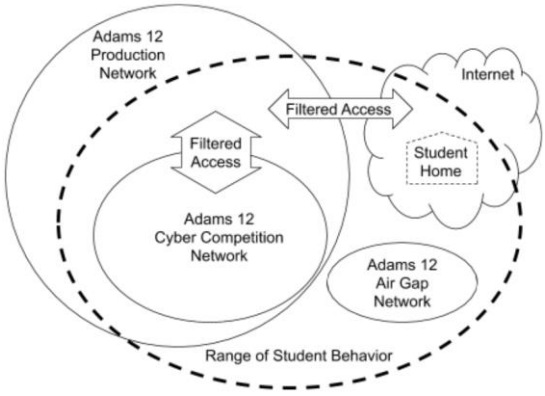

Fig. 2. Range of Encouraged Behavior at Adams 12

The Production Network provides functions a general business and education network of the institution can be carried out, and which generally has physical and/or logical links to all departments of the institution, as well as to the broader Internet. Cybersecurity students use this for their normal classroom activities and for research in their cybersecurity courses. This migration of students raises the risk that learned behavior on the air gap network may transfer to the production network. This network has standard security configurations set up in response to contemporaneous threat analytics, but was not initially designed to support cybersecurity training activities.

As cybersecurity training was introduced for students, several additional options as a Cyber Competition Network were required because students needed access to administrative controls over computers and network devices in order to gain the skills for learning and for competition. Adams 12 provisioned designated machines on a Guest network that still allowed students to connect to the CyberPatriot scoring engines on the Internet, while eliminating peer-to-peer activities. As the network engineer reviewed required activities, this pre-existing network matched the required access closely. However, the Guest Network had to be deployed manually to student computers in Pods, switching from the Production Network for each competition. Therefore, a dedicated Cyber Competition Network is being planned to remove the manual process and allow for security controls customized to cyber competitions. Provisioning a dedicated network should also help supporting CyberPatriot programs across multiple sites as the competition becomes more popular. The competition computers are dedicated to the CyberPatriot students and Adams 12 pre-loads them with virtualization software that runs the as a virtual PC. These machines also have a different security posture with a unique local administrator password, and hardware-protecting password.

To support both the cybersecurity curriculum and the CyberPatriot program with training experiences proven out on actual computer and network hardware, the team designed an Air Gap Network that could operate as a sandbox for students to experiment with systems, network devices. This is a place where students can be encouraged to try things even if they have a chance of breaking, and work to fix them with-

out consequences. This network does not have any wireless devices, and is located away from open network jacks. Any devices containing wireless electronics needed in the Air Gap Network have their wireless devices disabled at the BIOS layer before they are added. The Air Gap Network also includes warning labels about connection and has a significant distance or "air gap" between these devices and any connection to other Adams 12 networks.

5.3 Ethical Training and Adjudication

A significant part of mitigating the school district's risk is establishing a formal consent relationship with parents and students that transparently describes the skills students will learn, the activities they engage in, and the knowledge they will gain. While parents must sign a form consenting to the activities, a structured set of meetings begins prior to the course and proceed through the first quarter of the course session. This category covers both where students experience control of behavior based on policy and also walk through scenarios to learn self-control later on in life.

When discussing the syllabus with the students, teachers set class behavioral expectations. These expectations include logging off of the computer before leaving the classroom for the day. If a student fails to log out of the computer and another student in the next class period goes to the computer to work on it, the expectation is for that student to log out the previous user and log into their own account. Any student who is caught working on a computer logged into another student is written up. If it happens more than one time students can lose lab access. Then, they have to hand write everything, including any code for the programming classes. Academic honesty is also discussed when discussing the syllabus, but this is general to all coursework.

5.4 Limits on Teaching Risky Content Areas

The Adams 12 cybersecurity coursework currently sets limits on content, particularly hands-on activities. This is an acknowledgement that skills taught in the cybersecurity curriculum can create risks for children if they acquire skills and habits that translate readily into inappropriate, disruptive, or illegal activities. Exclusions include things like scanning networks, working with malware, and some scripting activities.

While current technical controls help reduce these risks when students are on Adams 12 networks, the school district leadership understands that the student takes cybersecurity skills with them into a broad range of technology environments at home, at the library, and at other institutions. Limiting content is also a protection measure because students daily migrate from the Challenge Network environment to the computers on Adams 12's production network that is used for their other classes.

6 Analysis

One thing that became apparent in case review is that the risk reduction measures were prompted by the level of engagement of student content. Students learning how

to harden a system were less likely to be disruptive or to misuse the skills they had acquired, either on the network or in the larger community. A matrix of levels along with the original risk reduction categories makes the discrete work at each level clearer, and provides a context for the type of prompts that might lead to these risk reduction measures. We designed the matrix, shown in Table 2, with the expectation that it could be used to track institutional cyber resilience in relation to both the presence of cybersecurity education programs generally, and the practices within the risk reduction categories.

One obvious factor that came up with Regis was the need to completely mitigate the network risk associated with outreach programs to children. The isolation of laptop machines removed the need for internet filtering, eliminated peer-to-peer digital behavior, and reduced dramatically the threat of malware or malicious network activity. At Adams 12, significant effort goes into maintaining a safe and secure environment for children with multiple isolated networks directly addressing concerns related to children. Therefore, the boundaries in Table 2 between levels 3 and 4 is a strong boundary for consideration. Children, levels 1-3 require significant constraints on the actual content, and strong involvement of parents. Adults, at Regis, required strong institutional relationships through agreements or sponsoring staff, while placing significant emphasis on the adherence to professional ethical guidelines of aspiration or affiliation. Each cell within Table 2 provides a defined point of reference designed so that a rating of risk coverage can be applied as a way of highlighting areas across the institution and cybersecurity program where curricular overreach creates risk beyond standard cybersecurity threat assessment.

Table 2. Matrix of Cybersecurity Deployment

L	Level Title	Groups	Curricular Limits	Technical Controls	Ethical Engagement	Institutional Behavioral Policy
1	Theory and basic skills	Minor and adult college/ Prof. Dev.	Password security, cryptography, least permission, privacy, ethics, and law (No scan or scripting tools)	Network segmentation, edge firewalling, competition computer hardening	Meetings with parents and students prior to the course	Institutional policy, parental permission for extracurricular,
2	Systems defense	Minor and Adult College/ Prof. Dev.	Endpoint Protection and patching, System Hardening, Permissions, Unauthorized Access Response. (No scanning or scripting tools)	Network Segmentation, Edge, Host & East-West Firewalling, competition computer hardening	Mid-class parent meetings, technical explanation of student skills and capabilities	Institutional policy, parental permission for extracurricular,
3	Network defense, system Investigation and alerts	Minor and Adult College/ Prof. Dev.	Firewall rules, forensics with autopsy. (No scanning tools)	Network forensics, device monitoring, log analysis and reporting.	Parent participation encouraged as a part of awareness building.	Institutional policy, parental permission for extracurricular,
4	Service attack/ defense	Adult College/ Prof. Dev.	No construction of Malware or active Internet-based attacks	Isolation of Laboratory Environments, Layer 7 Firewalling.	Institutional Computer Usage Agreement, Course-embedded Ethical and Policy Content	Student identity confirmation. visiting students must have institutional liability insurance and a responsible guest faculty member.
5	Process attack/ defense	Adult College/ Prof. Dev.	No targeting proprietary or operational systems: Financial software, etc. or weaponizing	Whitelist-only web application firewalling	Engage through professional societies, employers, partner institutions, and certifications	Invitation or approval only for current practice.

7 Conclusion

Because of the increasing societal need for cybersecurity education and training programs, regularizing and formalizing the risk mitigation methods that are needed to keep these programs running smoothly is becoming more significant. While the matrix for risk reduction presented here is developed on two cases that span across, public education of children, university level education, and professional training, it is likely that two customizations of this matrix will need to occur if others intend to use it. First, technology content changes over time, as does the expectations of learners at various levels, so the content will need to be adapted. Second, the threatscape that all institutions face regardless of their curricular content is advancing, so more lower level risk controls will become redundant with the institutions baseline of cybersecurity controls and risk reduction.

Another important implication of doing this work well, is that a matrix like this can help institutions address shortages of educators at all levels. The risks addressed here are not just institutional and societal risks. To make potential educators, parents, and students comfortable participating and contributing, we must find proactive and comprehensive ways to reduce their risk. Otherwise this becomes a high barrier for those considering entry into the field. Table 2 represents at least a framework for this consideration that is leveled to various learning environments.

8 References

1. Marcum, C., Higgins, G., Ricketts, M., Wolfe, S.: Hacking in High School: Cybercrime Perpetration by Juveniles, Deviant Behavior, 35:7, pp. 581-591, Taylor & Francis (2014).
2. Marquardson, J., Gomillion, D.: Cyber Security Curriculum Development: Protecting Students and Institutions While Providing Hands-On Experience. Information Systems Education Journal, 16(5) pp 12-21 (2018).
3. Boylan, A., Tepe, A., Davis, D.: Texas Governance and Authorities for Cyber Attack Response: A Summary, https://cybersecurity.tamu.edu/wp-content/uploads/2019/11/Cyber-Response-State-Authorities_13-NOV-19.pdf, last accessed 2020/7/3.
4. Fujs, D., Mihelič, A., and Vrhovec, S.: The power of interpretation: Qualitative methods in cybersecurity research, Tile of a proceedings paper. In: 14th International Conference on Availability, Reliability and Security (ARES '19), Association for Computing Machinery, New York, NY, USA, Article 92, 1–10 (2019).
5. Creswell, J., Creswell, J.: Research design: Qualitative, quantitative, and mixed methods approaches, p. 7, Sage publications (2017).
6. Carl D. Perkins Career and Technical Education Act of 2006, Public Law 88-210; December 18, 1963, As Amended Through P.L 116-6 Enacted February 15, 2019, United States of America (2019).
7. Knowles, M., Holton III, E., & Swanson, R.: The adult learner, Routledge, (2012).
8. https://www.acm.org/code-of-ethics, last accessed 2020/02/10.
9. National Collegiate Cyber Defense Competition Rules Page, https://www.nationalccdc.org/index.php/competition/competitors/rules, last accessed 2020/02/10.

10. Rocky Mountain Collegiate Cyber Defense Competition, https://plantzmasters.net/rmccdc/, last accessed 2020/02/10.
11. Cryptologic Foundation Framework, https://cryptologicfoundation.org/visit/goal/cybersecurity-curriculum-framework-portal-login.html, last accessed 2020/02/10.
12. Stallings, W., Brown, L., Bauer, M., Bhattacharjee, A.: Computer security: principles and practice, pp. 978-0, Pearson Education, Upper Saddle River, NJ, USA, (2012).
13. NICERC Cybersociety Curriculum, https://nicerc.org/curricula/cyber-society/, last accessed 2020/02/10.
14. Clark Center Home, https://www.clark.center/home, last accessed 2020/02/10.
15. NIST Cybersecurity Framework, https://www.nist.gov/cyberframework, last accessed 2020/7/3.
16. Nieles, M., Dempsey, K., Pillitteri, V.: NIST Special Publication 800-12 Revision 1 An Introduction to Information Security, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf, last accessed 2020/07/3.
17. Lockheed Martin Cyberquest™ Competition, https://www.lockheedmartin.com/content/dam/lockheed-martin/eo/documents/CyberQuest/2019/LM-CYBERQUEST-Challenge-Overview_PIRA.pdf, last accessed 2020/02/10.