# Cybersecurity Materials for K-12 Education

Kendall E. Nygard, Md Minhaz Chowdhury, K. Kambhampaty, and Pratap Kotala
Department of Computer Science
North Dakota State University
Fargo, ND 58103
{Kendall.Nygard, Md.Chowdury, K.Kambhampaty, Pratap.Kotala}@ndsu.edu

## Abstract

The role played by academic institutions in fulfilling the need for cybersecurity professionals is critical. At North Dakota State University, we are systematically increasing our educational efforts in providing cybersecurity education, including the establishing of an Institute for Cybersecurity Education and Research. One element of our efforts is reach into K-12 education, in an effort to interest and educate youth in cybersecurity. Through these efforts, we expect that there will be increased enrollments in cybersecurity programs at the technical college and university levels, helping to meet the demand for cybersecurity professionals. In this paper we discuss the structure of our cybersecurity materials developed for middle and high school students. Some of the materials were prototyped in programs offered in summer camps in 2016 and 2017 and are being expanded for summer offerings in 2018. Some of the camps were focused on Native American or female students. Topics include skills and tools for personal security and secure communication. We followed principles of educational theory, such as Bloom's taxonomy and recognizing learning styles in the development of materials. In the exercises, students were given instructional handouts, in class presentations and hands-on lab assistance. In this paper we discuss the content delivered and teaching methodologies that were utilized.

# 1 Introduction

Cyber-crimes cost the world nearly $3 trillion in 2015, a figure that is expected to rise to $6 trillion by 2021[1]. The cyber-crimes ranged from damage of data to fraud to loss of productivity. Cyber security breaches may be increasing by 27.4% per year[2]. This increase in cyber damages dramatically increases the demand for cybersecurity professionals. It is estimated there is already in 2018 a shortage of at least 350,000 cybersecurity professionals [3]. Unfilled positions in cybersecurity are expected to greatly increase to around 3.5 million by 2021[3].

Academic institutions are playing a critical role in increasing the number of professionals pursing cyber security education. At North Dakota State University, we are systematically increasing our educational efforts in providing cybersecurity education, including the establishing of an Institute for Cybersecurity Education and Research. One wing of our effort is to engage and interest K-12 students in cybersecurity. The effort is expected to stimulate cybersecurity program enrollment in higher education.

In this paper we discuss the structure of our cybersecurity materials developed for middle and high school students. The materials were prototyped in programs offered in the summers of 2016 and 2017 and are being expanded for 2018. The educational materials for these programs were developed incrementally and systematically, following the guidelines of most learning processes guided by. Bloom's Taxonomy and active learning strategies. This paper presents the background of such learning processes, the designed course content and the application of these learning processes.

The remainder of this paper is organized as follows: Section 2 describes the learning processes that we followed. Section 3 describes delivered course content, including the structure of the cybersecurity course materials. Section 4 describes obstacles to applying learning processes and approaches to address them. Section 5 describes the implementation and some results. Section 6 describes how the learning methodologies described in section 2 is reflected in the materials described in section 3. Section 7 provides details of a specific learning methodology subtopic. Section 8 concludes this paper by describing learnings from the past two summer camps and a plan for the upcoming summer camp.

# 2 Learning Processes

## 2.1 Bloom's Taxonomy

Bloom's taxonomy was created to design a learning process[4]. Following this taxonomy, there all three domains of learning: cognitive, affection and psychomotor.

The cognitive domain refers to the knowledge we acquire i.e. the mental skills. The opposite of this is psychomotor, which concerns mastering physical skills. Driven by repeated physical activities, a person can improve their skills. Affective learning refers to an evolution of emotions and attitudes.

The cognitive domain has attracted much attention. This domain is frequently used in curriculum design and development. This domain has six steps. These steps or levels can be represented using a pyramid shape (Figure 1). The bottom level of this pyramid is Knowledge. As we go up with the pyramid, it is assumed that the learner has already mastered the previous level. For example, starting from the Knowledge step, transition to the Comprehension step is achieved only when the first step is mastered.

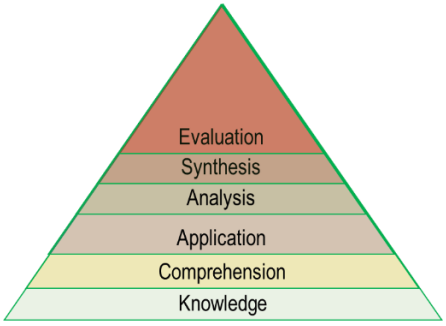


Figure 1: Bloom's Taxonomy

Also, each of the levels has their own goals. For example, the Knowledge level has a goal of remembering the fundamental information related to the topic of concern. For cyber security education the goal of this step is to teach learners the terminology and fundamental information related to the specific cybersecurity subtopics. In teaching cybersecurity, we view the Knowledge level in correlation with specific topics that can be explored and practiced in laboratory settings.

Table 1 covers each level of Bloom’s Taxonomy, including useful verbs that have been identified [5], and sample questions for each of the levels. This table also lists sample activities related to cybersecurity education as it applies to the cryptology topic area. Instructor can ask the learners to perform these types of activities.

| evel | Description | Useful Verbs | Possible activities/questions |
|---|---|---|---|
| Knowledge | The focus in this step is remembering information. In this step the questions shall be in such a way that the learner will be able to answer without any analysis. This level primarily deals with facts. | List, name, define, label, state, match, recognize, select, locate, memorize, recall, tell, enumerate, observe, read, record, retell, visualize [5] | 1. Learn the concept of an encryption key and what the key information is for some basic encryption examples.<br>2. Learn the operation and names of certain simple encryption/decryption algorithms.<br>3. Demonstrate that you remember the names and operations for some basic encryption methods.<br>4. Learn about some basic types of attacks, such as eavesdropping and denial of service? |
| Comprehension | Focus is developing the skill to demonstrate the ideas learned from the previous step. | Infer, relate, restate, translate, cite, generalize, give example, illustrate, group, show, rewrite, review, research, report | 1. What are the main characteristics that make the Caesar Cipher work?<br>2. How was cryptography used in the civil war? How about in World War II? |
| Application | Applying the knowledge learned in the first level in new situations | Modify, use, calculate, change, experiment, sketch, complete, paint, prepare, produce, articulate, act, collect, compute, | 1. Encrypt or decrypt a message using the Vigenere cipher.<br>2. Set the inputs and run the computer program that implements the Caesar Cipher. Learn how the operation differs for different keys. Explain what is involved in breaking a code sent using the Caesar Cipler. |

| | | | |
|---|---|---|---|
| | | operate, practice, predict, schedule, simulate, write | |
| Analysis | Identifying and explaining the relationship between the components of the topics covered in the Knowledge level. | Analyze, classify, infer, distinguish, separate, select, connect, divide, point out, prioritize, conclude, correlate, criticize, deduce, dissect [5] | 1. Learn how the Vigenere cipher works. Read about how the Vigenere cipher was used in the Civil war.<br>2. Explain what would be involved in breaking a code message that is encrypted using the Vigenere cipher.<br>3. Compare the Caesar cipher with the Vigenere cipher in terms of the work involved in deciphering a message. In your comparison, comment on how secure each method would be in practice. |
| Synthesis | Organizing elements from to generate a new product or process | Design, compose, create, plan, combine, invent, hypothesize, compile, develop, modify, organize, prepare, produce, rearrange, adapt, anticipate [5] | 1. Design a step by step process to decrypt a Caesar Cipher text.<br>2. We have a computer program with source code in Python for encrypting a message using the Caesar cipher. Explain each step of the code.<br>3. Based on your understanding of the Python code for the Caesar cipher, explain how the calculation part of the code could be modified to decrypt a message. |
| Evaluation | Evaluating and insightfully critiquing information | Criticize, evaluate, judge, support, compare, decide, recommend, | 1. In your own words, summarize the advantages and disadvantages of the Caesar cipher and the Vigenere cipher? |

| | | | |
|---|---|---|---|
| | | discriminate, assess, convince, defend, measure, rank, score, deduce, dissect [5] | |

Table 1 Bloom's Taxonomy Cryptography Examples

## 2.2 Revised Bloom's Taxonomy

The revised Bloom's taxonomy renamed the levels of steps with verbs rather nouns[6][7][8][9][10][11]. For example, the revision changed the bottom level "Knowledge" into "Remember". Level 5, Synthesis, is replaced by Evaluate and level 6, Evaluation is replaced by Create. Create is defined as combining or organizing the learned elements into something new that is functional. Figure 1 compares the two taxonomies.

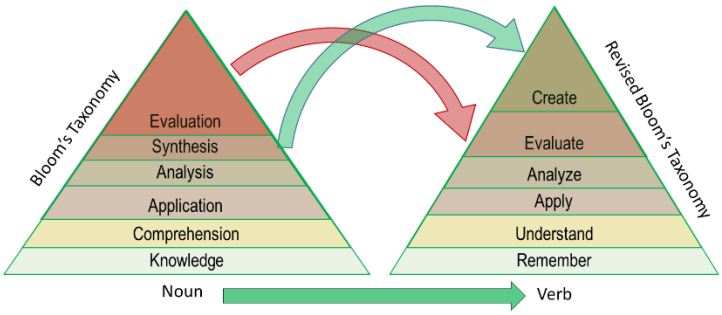


Figure 2 Original vs Revised Bloom's Taxonomy

## 2.3 Learner Engagement in Class: Active Learning

### 2.3.1 Active learning, learning strategies and obstacles

Active learning is a way to stimulate learning by engaging students in performing activities [12][13][14][15]. Meyers and Jones defined active learning as "Active learning is a style of learning that provides opportunities in the classroom for students to talk, listen, read, write and reflect as they engage in a variety of learning activities. These activities include such things as answering questions, solving problems, analyzing and discussing case studies, analyzing and commenting on printed or other materials [12].

Bonwell suggested active learning strategies, mentioned below [13]:

1. Instructor shall provide instructions for activities for which learners are involved in doing something, and also thinking about what they are doing. In our cybersecurity activities, we provided step by step instructions with photo descriptions of how to practice a certain learning topic.

2. Learners shall read, write, discuss or engaged in problem solving. Learners read or listened to our instructions, wrote the solution in a paper after solving a given cryptology problem.
3. Learners shall be involved in Analysis, Synthesis and Evaluation. Learners read a python code we provided, received instruction them on the details of analyzing the encryption formula in the code, and had them provide input and run the code online. In another exercise, they used online descriptors of the steps of a Caesar cipher code and evaluated the performance of this encryption algorithm.

We are also presenting a partial list of other active learning strategies [14][15].

1. Showing a pictorial illustration of a topic in class. We described the security issue of message transfer using pictures with Alice and Bob exchanging messages [16].
2. Breaking the lecture into parts. During each breakpoint the learner crosschecks their notes with his/her fellow learner. Each of our one-hour class was divided into lecture listening, problem solving sessions with a pause between those sessions.
3. Time management. Allowing sufficient time after asking for the solution of a question to the learner.
4. Choral response. asking a comprehensive question in class, so that all learners can think about the answer and correct themselves if they are wrong. The question we asked in our class was “Has anybody heard about digital certification?” “
5. Volunteers. Choosing a volunteer to get involved by asking questions. We gave a project to the learners asking them to describe a way to sending a secured message with some preconditions. We utilized two learners playing the role of Alice and Bob to demonstrate the problem.
6. Socratic questioning. Asking a learner a question in such a way that the answer leads to the next topic to be discussed. An example is asking the learner “Does anybody wanted to send a message to only one of your friends in such a way that other friends will be able to read the message but will not able to find its meaning”. This type of question served to introduce our cryptology topic. Two more examples are ”Why do you think you need good a password?”, ”Why it is not a good idea to make a username and password identical?”.
7. Problem solving by the learner. Example, learners encrypted a text using Caesar cipher.
8. Coding. learners ran a provided Python code and observed the result and analyzed the code to learn how they can implement an encryption algorithm.

Some known obstacles to active learning are given as follows [13]:

1. Accommodating the learning content in the available class time.
2. Preparation time can be longer than estimated.
3. Larger classes can be difficult for applying active learning.
4. Lack of learning resources.

In our cyber security educational effort, we applied strategies from both Bloom’s Taxonomy and active learning activities while overcoming many of the obstacles shown in **Error! Reference source not found.**.

# 3 Delivered Course Content: Structure of the Cybersecurity Course Materials

During the design of the course materials, the application of Bloom's Taxonomy and active learning principles were goals. Table 2 illustrates the structure of several the cybersecurity educational materials. In this table, the second column is the cybersecurity topics covered, the first column describes the activity summary related to that cybersecurity topic, third column indicates whether a Classroomroom setting or lab was employed, and the last column provides details of the activity related to each topic.

| Activity | Topics covered | Activity place | Activity Details |
|---|---|---|---|
| Presentation on Identity Theft, Cryptography, Trust | Data breach | Classroom | Examples of data breach and associated monetary loss. |
| | Scenarios that can happen during message transfer between two people | Classroom | 1. Lecture: power point slide demonstration with Alice and Bob characters was shown. |
| | | Lab | 2. Student Project: demonstration of secured message transfer project problem, given to student to solve, with two students as volunteers. |
| | Elementary encryption algorithms | Classroom | 1. Freemason cipher |
| | | | 2. Secret key encryption |
| | | | 3. Caesar Cipher |
| | | | 4. Vigenere Cipher. |
| | Cryptology in USA history | Classroom | 1. Civil War (battle of Vicksburg) used encrypted messages. |
| | | | 2. Assassination of President Abraham Lincoln: Vigenere cipher text was found at the assassin's possession. |
| Using an online Password Cracker | Demonstration of password strength | Lab | Step 1: students encrypted a password using an online facility where students were able to choose a certain encryption algorithm. |

| Activity | Topics covered | Activity place | Activity Details |
|---|---|---|---|
| | | | Step 2: students then put this encrypted password into an online password cracker. Students observed the time requiring to crack a password. This time implied the strength of a password.<br><br>Detailed step by step instruction handout on how to use such tools and how to observe the time difference were provided. |
| Working with an Online Vault Password Manager | Password management | Lab | Step 1: students saved several passwords in a password vault by installing this vault into the lab's computer. |
| | | | Step 2: they created accounts on different suggested web sites and then saved the passwords into this vault.<br><br>Observation is that when they next time they logged into these sites, the passwords were already saved and students didn't need to type password again. |
| Working with a Password Generator | Generating secured password | Lab | Step 1: students installed a browser extension (recommended in the instruction) and used their own given master password to login into that extension. |
| | | | Step 2: they used this extension to generate password for a website. |
| | | | Step 3: at the same time this extension saved the login credentials (using the generated password) needed to login into that website. |
| How to use anti-virus and online resource identifying malware | Malware | Classroom | Step 1: malware, their history and short description were presented. |
| | | Lab | Step 2: students observed an installed anti-virus software e.g. windows |

| Activity | Topics covered | Activity place | Activity Details |
|---|---|---|---|
| | | | defender reactions by following step by step instructions. |
| | | | Step 3: used online resources e.g. virus total to look for potential malware into files and URLs. |
| Test web browser security | Web browser security | Lab | Step 1: Students scanned the Chrome and Firefox web browsers' vulnerability using a plug-in. |
| | | | Step 2: They fixed the existing issues (by following our given instruction handout) with these browsers using this plug-in's facility. |
| Manage locally shared object to reduce the browser security breach possibility | Web browser security: locally shared object | Lab | Students learned ways to manage the information website stores in local shared objects e.g. changing storage limit of a website, removing data for a website. |
| Configuring web browser security settings | Web browser security settings | Lab | Students configured the security settings for the Google Chrome, as instructed. Examples of such setting are removing cookies, clearing browsing data, preventing java script to be run by any sites, permission to run plug-in of any sites. |
| | | | Students first observed the browser behavior before applying these settings and then applied the settings to observe the affect or aftermath of these settings change on the browser. |
| Steganography | Steganography | Lab | Step 1: students hid a message in a picture using software called OpenPuff. |
| | | | Step 2: they retrieve the same message from the picture using OpenPuff. |

| Activity | Topics covered | Activity place | Activity Details |
|---|---|---|---|
| Trace route of a web site using both command prompt and online trace route resource | Tracing route of a web site | Lab | Step 1: students ran command prompt following instructions. The goal is to locate the IP address of the machine they are currently working on. They used both command prompt and online resources addressing this ip address. |
| | | | Step 2: students were able to trace route of few web sites using both command prompt and online trace route resource. |
| Creating and Using QR Codes | QR codes security flaw | Lab | Step 1: students created a QR code for their own home address using a mobile app. |
| | | | Step 2: they then sent the QR code via email. |
| | | | Step 3: they retrieved the QR code and the address from the code realizing the security flaws of using QR code. |
| Learning possible secure ways of communicating over internet | secure communication | Classroom | A scenario was presented in class showing safe and secured communication ways over the internet following the concepts taught in the summer camp. |

Table 2 Structure of the cybersecurity course materials

# 4. Obstacles to Learning Processes and Solutions

During the application of Bloom's Taxonomy and active learning in course design, we faced the following obstacles:

1. Accommodating the learning content in available class time: To overcome this obstacle, during the course design we introduced topics related to a person's daily life activities. For example, if we put a section on cloud security, then the high school students may fail to correlate this incident with their daily life activities. Hence, we covered only topics related to personal security and secured communication.
2. Lack of learning resources: As we were using the North Dakota State University's computer system, few cyber security topics were not straightforward to demonstrate. Example is the demonstration cyberattacks using software e.g. Wireshark. Hence, we excluded cyberattacks demonstration in our activity oriented learning.

3. A larger class is difficult for applying active learning: To overcome this obstacle, in all the exercises students worked out, they were given step by step pictorial instruction handouts, in class power point presentations and assistances in lab. The assistance rate was approximately 1 instructor for every 10 students.

In the later sections, the Bloom's Taxonomy levels application and the active learning application are described. Since it is not feasible to present all the content of topics, only one of the content areas are described in detail.

# 5. Teaching Methodologies for Learning Engagement

We applied Bloom's Taxonomy in the two summer camp programs. In most of the levels we were able to deploy active learning strategies. However, we were not able to support the Analysis and Evaluation levels of the Taxonomy.

## 5.1 Knowledge

In this level, the terminology plays a big role. In our summer camp handouts, important terms were highlighted e.g. we used them as captions to subsections or used a bold font. As mentioned earlier, scenarios were used describing a topic both in the class and the lab. For example, the often employed characters Alice and Bob were used to demonstrate various issues of confidential message transfer. Scenarios were described using graphics and animations. The terminologies were also highlighted in such scenario descriptions. We also used pictorial descriptions for most concepts.

During the questionnaire to the learners, we made sure they can connect to the topics e.g. concepts and characters that they have seen and learned from in the classroom. For example, two volunteer students were requested to assist by pretending one was Alice and other Bob to demonstrate the secured message transfer project problem. Alice and Bob characters were used in lectures describing the problem and solutions of secured message transfer. After completion of each subsection, short questions were asked. The way of asking question is also an implementation of active learning. Some example questions, are given below.

1. What are the primary digital certification methods?
2. Between the Caesar cipher and the Vigenere cipher, which one uses alphabet shifts?
3. When a false message is sent to Bob pretending it sent by Alice where Alice didn't send any, the source of the message is not authentic. What is the name of this attack?

## 5.2 Comprehension

Each topic taught has a transition time. This transition time can be a short pause or a question or a summary of the topic that was just described. A wise decision is to choose a question whose answer summarizes the whole taught topic or pin points important sub topics. Such question helps determining whether the student was able to understand the gist of the content. In the summer camps we asked questions during the transition time of

two topics to comprehend the topic we covered. Such questions kept the students active in the class about learning. Two sample questions are given below.

1. Do you think hiding your message using QR code is secure? Why or why not?
2. You have learned how to configure a web browser to make your browsing more secure. Do you now intend to use the default browser setting at home or will you configure them? Can you recall what the issues with web browser security?

### 5.3 Application

Many of the topics that correlate at the Knowledge and Comprehension levels need application level learning. This tends to engage the students into the course contents. Also they tend to gain interest in the topic. The students followed step by step instructions for each topic under the hood of this application level. These steps by step instructions they followed simulated the real life task they may need to accomplish in their future job. Hence, such instruction based learning in lab confirmed the engagement of active learning. Most of the topics from the summer camps were covered in this application level. Followings are the covered activities that ensures application level learning.

1. We have a message, can you encrypt it using Caesar Cipher method and shifting the characters by one?
2. Can you decrypt this message, given the key shift and the message?
3. Using an online password cracker to decode a password (in lab).
4. Working with online vault password manager (in lab).
5. Working with password generator (in lab).
6. How to use anti-virus and online resource identifying malwares (in lab).
7. Test web browser security (in lab).
8. Practice web browser security settings and configuration (in lab).
9. Trace route of a web site using both command prompt and online trace route resource (in lab).
10. Create and use a QR Code and observe the security issue of hiding message using QR code.

### 5.4 Synthesis

Synthesis level is the ultimate way to know how the learner will behave in a real life scenario that is not exactly what was taught in class. This level is crucial for computer science education as computer science problem solving needs to correlate with real life problems. In this level we gave students a project, during the last class. The project is about transmitting a message safely and securely over the internet. Students were advised to follow the concepts taught in the summer camp. This is equivalent to real life problem solving and hence confirm the involvement of active learning. The problem was described using two volunteers playing the role of Alice and Bob[16].

## 6. Details of Application Level Example

Students were given various tasks ranging from ‘examining data breaches’, ‘cracking password’, ‘online password vault manager’ etc. All the tasks were carried out in a windows based computer laboratory. One of the applications was Traceroute. Students were asked to do run Traceroute and utilize it as a diagnostic tool. Traceroute displays the path of packets across an Internet Protocol (IP) network as they move from source to destination and includes the mean time that packets required from one hop to another. Bloom’s taxonomy states that, ‘the ability to use learned material, or to implement material in new and concrete situations’.  Slightly differently, the revised Bloom’s taxonomy states “Carrying out or using a procedure through executing, or implementing. Applying relates to or refers to situations where learned material is used through products like models, presentations, interviews or simulations.” Instructions were provided for this task. The hands on experience from previous tasks helped the students gain an understanding the steps without the need for visual display. This co-relates to the Application level in Bloom’s taxonomy. Students from the ‘run command’ were able to navigate to a ‘command prompt’. From the command prompt, they were asked to find out the IP address of the computer they were using along with Traceroute of their favorite website. Students accomplished this task with verbal instructions. Figure *3* shows an example of the instructed task.

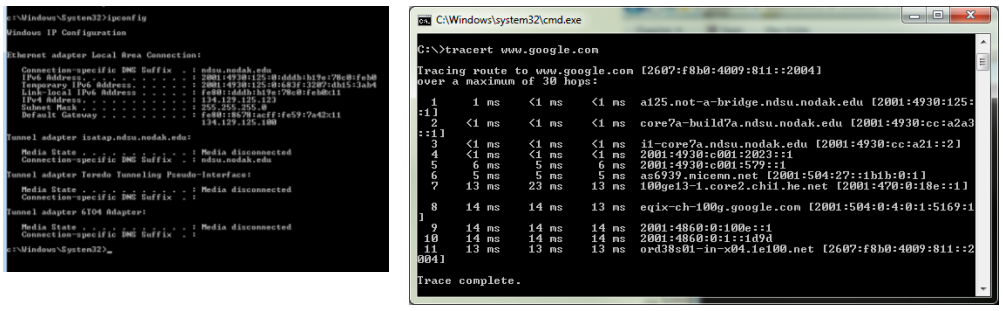


Figure 3 The IP Configuration and Traceroute from a command prompt

# 7. Conclusion and Future Plans

Bloom’s Taxonomy helped us to determine how well the students are learning. It also helped us to embed active learning with its different levels e.g. Knowledge, Synthesis and Application. The various levels of the taxonomy helped us identifying the missing sub topics in our last two summer camps and is helping in designing our future summer camp. We were able to compare the objective of each topic with the perspective of each student about that topic. This helped us in determining what else we need to change in future summer camp design. We plan to include tasks at the Analysis and Evaluation levels for the summer 2018 summer camp.

We also realized the limitations of our learning processes. We were able to overcome some of our resource limitation obstacles. For example, for the upcoming summer camp we will be providing the raspberry pi computers to each student. Using these small computers, we will be able to implement additional projects, add the missing sub topics and add new topics.

In addition, our Institute for Cybersecurity Education and Research has been awarded funding for the 2018 summer camp. Experience gained during the 2016 and 2017 summer camps allows us to refine our content and delivery approaches, guided by Bloom's taxonomy, learning styles, and methods of active learning.

# References


[1] Pierluigi Paganini, "Cost of cybercrime will grow from $3 trillion (2015) to $6 trillion by 2021Security Affairs." http://securityaffairs.co/wordpress/50680/cyber-crime/global-cost-of-cybercrime.html.

[2] Accenture, "Cost of cyber crime study 2017 insights on the security investments that make a difference," 2017.

[3] Steve Morgan, "Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021 | CSO Online." [Online]. Available: https://www.csoonline.com/article/3200024/security/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html. [Accessed: 16-Mar-2018].

[4] B. S. (Benjamin S. Bloom, *Taxonomy of educational objectives; the classification of educational goals,*. Longmans, Green, 1956.

[5] J. Dalton, D. Smith, and Victoria. Schools Division. Curriculum Branch., *Extending children's special abilities : strategies for primary classrooms*. Curriculum Branch, Schools Division, 1986.

[6] D. R. Krathwohl, "A Revision of Bloom's Taxonomy: An Overview," *Theory Pract.*, vol. 41, no. 4, pp. 212–218, Nov. 2002.

[7] L. Anderson, D. K.-… P. Artz, undefined AF, and undefined 2001, "A taxonomy for learning, teaching and assessing: A revision of Bloom's taxonomy," *nsee.memberclicks.net*.

[8] D. R. Krathwohl and L. W. Anderson, "Merlin C. Wittrock and the Revision of Bloom's Taxonomy," *Educ. Psychol.*, vol. 45, no. 1, pp. 64–65, Jan. 2010.

[9] M. P.-J. of F. and C. Sciences and undefined 2007, "The new Bloom's taxonomy: An overview for family and consumer sciences," *uncwweb.uncw.edu*.

[10] A. C.-T. & Learning and undefined 2008, "Bloom's taxonomy blooms digitally," *teachnology.pbworks.com*.

[11] T. Noble, *Integrating the revised bloom's taxonomy with multiple intelligences: A planning tool for curriculum differentiation, Teachers College Record (Vol. 106, pp. 193): Blackwell Publishing Limited.*, vol. 106, no. 1. 2004.

[12] C. Meyers and T. B. Jones, *Promoting active learning : strategies for the college classroom*. Jossey-Bass, 1993.

[13] C. Bonwell and J. Eison, *Active Learning: Creating Excitement in the Classroom. 1991 ASHE-ERIC Higher Education Reports.* 1991.

[14] M. Prince, "Does Active Learning Work? A Review of the Research," *J. Eng. Educ.*, vol. 93, no. 3, pp. 223–231, Jul. 2004.

[15] M. L. Silberman, *Active learning : 101 strategies to teach any subject*. .

[16] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.