Cybersecurity 120

October 11, 2019

New Nouveau Brunswick

2019
Department of Education and Early Childhood Development
Curriculum Branch

Acknowledgments

The Department of Education and Early Childhood Development of New Brunswick (EECD) gratefully acknowledges the contributions of the following groups and individuals toward the development of the New Brunswick Cybersecurity 120 (CYBER 120) curriculum document:

High School Cybersecurity Curriculum Development Committee:

- Natalia Stakhanova (UNB Computer Science and also CyberLaunch Academy)
- Kathy MacDonald (ASD-North)
- Janet Wilson (ASD-South)
- Jeremy Brown (ASD-West)
- Carl Legere (ASD-West)
- Adam Binet (ASD-East)
- Ryan Murphy (ASD-South)
- Andrew Colwell (EECD)

Cybersecurity 120 Piloting Committee:

- Nick Fullerton (ASD-North)
- Joel Flannagan (ASD-East)
- Toller Pope (ASD-East)
- Ben Kelly (ASD-East)
- Cynthia Leblanc (ASD-South)
- Janet Wilson (ASD-South)
- Peter Woytiuk (ASD-South)
- Geordie Doak (ASD-South)
- Jeremy Brown (ASD-West)
- Carl Legere (ASD-West)

Graham Rich, Learning Specialist for Information and Communication Technology (EECD)

Many thanks to the following people for their essential roles in the creation of this course:

- Brian Gray (EECD and later Cyber NB), William Kierstead (CyberNB), and Heather MacLean (CyberNB)
- Ryan Murphy (EECD, seconded to support the rollout of the Cyber Defense Hub during pilot)
- Natalia Stakhanova (Professor and CyberLaunch Academy founder, for sharing her expertise and resources, handouts and presentations)

Table of Contents

1. Introduction

1.1 Mission and Vision of Educational System

The New Brunswick Department of Education and Early Childhood Development is dedicated to providing the best public education system possible, wherein all students have a chance to achieve their academic best. The mission statement for New Brunswick schools is:

> *Each student will develop the attributes needed to be a lifelong learner, to achieve personal fulfillment and to contribute to a productive, just and democratic society.*

1.2 New Brunswick Global Competencies

New Brunswick Global Competencies provide a consistent vision for the development of a coherent and relevant curriculum. The statements offer students clear goals and a powerful rationale for school work. They help ensure that provincial education systems' missions are met by design and intention. The New Brunswick Global Competencies statements are supported by curriculum outcomes.

New Brunswick Global Competencies are statements describing the knowledge, skills and attitudes expected of all students who graduate high school. Achievement of the New Brunswick Global Competencies prepares students to continue to learn throughout their lives. These Competencies describe expectations not in terms of individual school subjects but in terms of knowledge, skills and attitudes developed throughout the curriculum. They confirm that students need to make connections and develop abilities across subject boundaries if they are to be ready to meet the shifting and ongoing demands of life, work and study today and in the future.

See Appendix 6.1.

2. Pedagogical Components

2.1 Pedagogical Guidelines

Diverse Cultural Perspectives

It is important for teachers to recognize and honour the variety of cultures and experiences from which students are approaching their education and the world. It is also important for teachers to recognize their own biases and be careful not to assume levels of physical, social or academic competencies based on gender, culture, or socio-economic status.

Each student's culture will be unique, influenced by their community and family values, beliefs, and ways of viewing the world. Traditional aboriginal culture views the world in a much more holistic way than the dominant culture. Disciplines are taught as connected to one another in a practical context, and learning takes place through active participation, oral communication and experiences. Immigrant students may also be a source of alternate world views and cultural understandings. Cultural variation may arise from the differences between urban, rural and isolated communities. It may also arise from the different value that families may place on academics or athletics, books or media, theoretical or practical skills, or on community and church. Providing a variety of teaching and assessment strategies to build on this diversity will provide an opportunity to enrich learning experiences for all students.

Universal Design for Learning

The curriculum has been created to support the design of learning environments and lesson plans that meet the needs of all learners. Specific examples to support Universal Design for Learning for this curriculum can be found in the appendices. The **Planning for All Learners Framework** will guide and inspire daily planning.

See Appendix 6.2

English as an Additional Language Curriculum

Being the only official bilingual province, New Brunswick offers the opportunity for students to be educated in English and/or French through our public education system. The EECD provides leadership from K-12 to assist educators and many stakeholders in supporting newcomers to New Brunswick. English language learners have opportunities to receive a range of instructional support to improve their English language proficiency through an inclusive learning environment. EECD, in partnership with the educational and wider communities offer a solid, quality education to families with school-aged children.

2.2 Pedagogical Guidelines

Assessment Practices

Assessment is the systematic gathering of information about what students know and are able to do. Student performance is assessed using the information collected during the evaluation process. Teachers use their professional skills, insight, knowledge, and specific criteria that they establish to make judgments about student performance in relation to learning outcomes. Students are also encouraged to monitor their own progress through self-assessment strategies, such as goal setting and rubrics.

Research indicates that students benefit most when assessment is regular and ongoing and is used in the promotion of learning (Stiggins, 2008). This is often referred to as formative assessment. Evaluation is less effective if it is simply used at the end of a period of learning to determine a mark (summative evaluation).

Summative evaluation is usually required in the form of an overall mark for a course of study, and rubrics are recommended for this task. Sample rubrics templates are referenced in this document, acknowledging teachers may have alternative measures they will apply to evaluate student progress.

Some examples of current assessment practices include:

• Questioning	• Projects and Investigations
• Observation	• Checklists/Rubrics
• Conferences	• Responses to texts/activities
• Demonstrations	• Reflective Journals
• Presentations	• Self and peer assessment
• Role plays	• Career Portfolios
• Technology Applications	• Projects and Investigations

Formative Assessment

Research indicates that students benefit most when assessment is ongoing and is used in the promotion of learning (Stiggins, 2008). Formative assessment is a teaching and learning process that is frequent and interactive. A key component of formative assessment is providing ongoing feedback to learners on their understanding and progress. Throughout the process adjustments are made to teaching and learning.

Students should be encouraged to monitor their own progress through goal setting, co-constructing criteria and other self-and peer-assessment strategies. As students become more involved in the assessment process, they are more engaged and motivated in their learning.

Additional details can be found in the Formative Assessment document.

Summative Assessment

Summative evaluation is used to inform the overall achievement for a reporting period for a course of study. Rubrics are recommended to assist in this process. Sample rubrics templates are referenced in this document, acknowledging teachers may have alternative measures they will apply to evaluate student progress.

For further reading in assessment and evaluation, visit the Department of Education and Early Childhood Development's Assessment and Evaluation site here.

Cross Curricular Literacy

Literacy occurs across learning contexts and within all subject areas. Opportunities to speak and listen, read and view, and write and represent are present every day -in and out of school.

3. Subject Specific Guidelines

3.1 Rationale

The field of cybersecurity has evolved significantly, especially in the past decade. This Cybersecurity 120 curriculum is a first for New Brunswick and seeks to bridge the gap between key components in student learning, as specified by representatives from industry and post-secondary education.

During this program of study, students will be challenged through the lens of project-based learning. The curriculum outcomes demonstrate the commitment to New Brunswick's implementation of 'Global Competencies'. Through the collaborative projects in this course, students work towards these outcomes in learning activities that are meaningful and focused on the student. These Global Competencies should not be interpreted as instructional pathways but rather expectations to be met simultaneously with the skills and knowledge required in this course.

The required knowledge and specific skills shown in the SCO's have been limited in quantity, to facilitate students' deeper investigation and application of the curriculum topics, while also providing flexibility for instructors as the field of cybersecurity has shown surprising shifts over short amounts of time.

The primary purpose of this course is that students will demonstrate operational skills and will use computational thinking to solve problems and to analyze cybersecurity challenges with an eye to mitigating risks.

3.2 Course Description

The Cybersecurity 120 (CYBER120) course will inspire students through the experiential learning of the fundamentals and possibilities of cybersecurity. In Cybersecurity 120, students will be actively engaged in the design, development and evaluation of defensive cybersecurity projects, including awareness, concepts and challenges. The intent of this program of study is to have students discussing real-world case studies and learning in hands-on activities from day one, while maintaining a high level of engagement throughout the course through a commitment to problem-based and project-based learning. To achieve a high level of student engagement, teachers will use a feedback loop of instruction, hands-on learning, and assessment. See example below:

Present one fundamental aspect of cybersecurity (e.g. firewalls).

- What is the *computational thinking* behind it? (e.g. how a firewall works, involving pattern recognition, algorithmic thinking, decomposition and abstraction)
- What planning surrounds this? (e.g. how to position a firewall in a network)
- What *security* and *implementation* strategies does this require (e.g. knowledge and use of ports)
- How is this *used in my project*? (e.g. explain where, why and how a firewall will be deployed)
- Has the student demonstrated knowledge and use in an *assessment*? (e.g. deployed correctly)

It is recommended that teachers introduce cybersecurity concepts through real-world case studies and hands-on activities that are based on problems, challenges, and projects that become increasingly open ended. These open-ended challenges avoid a single correct answer and instead have students weigh the benefits, costs, risks, precedents, consequences, and side-effects in complex situations.

For teachers fostering interest in cybersecurity, students will be entering the stream of study at various starting points with differing levels of experience and competence; therefore, teachers will need to adjust the learning activities and student groupings in order to reach students where they are. For instance, some students may have cybersecurity experience from extra-curricular teams and clubs (including CyberTitan) or from curricular opportunities in elementary school, in Middle School Technology Education (MSTE), or in Broad Based Technology 9/10 (BBT).

To aid in teacher awareness, some potential paths of cybersecurity background and experience are highlighted below:

High Level of Experience	**Medium Level**	**Low Level**
Elementary School • Introduced to citizenship and cybersecurity concepts and case studies	Elementary School • None	Elementary School • None
Middle School • Complete citizenship and cybersecurity module in *MSTE* • Member of a CyberTitan extra-curricular team	Middle School • Complete citizenship module in *MSTE*	Middle School • None
High School • Complete citizenship and/or cybersecurity modules in *BBT 9/10* • Complete *Cybersecurity and Technical Support 110* • Member of a CyberTitan extra-curricular team • Enrolling in *Cybersecurity 120*	High School • Complete citizenship and/or cybersecurity modules in *BBT 9/10* • Complete *Cybersecurity and Technical Support 110* • Enrolling in *Cybersecurity 120*	High School • Enrolling in *Cybersecurity 120*

By the end of this course, students will have an awareness, understanding and experience with cybersecurity, especially in the context of vulnerability identification and assessment, defensive strategizing, risk mitigation, and the forensic removal of cybersecurity threats.

3.3 Safety Guidelines

Students will be learning about real world events and criminal activities. Students should be made aware that the illegal events are not to be glorified nor implemented, other than for the purpose to prevent such events. No activities will contravene Policy 311.

At this point in the development of cybersecurity education within the public school system of New Brunswick, our focus has entirely been defensive, as students are involved in forensics, vulnerability analysis, case studies, securing and safeguarding computer images and networks, and similar activities.

In the future, there may be opportunities for students to learn offensive cybersecurity skills, including *ethical hacking*, largely based on the skill set and activities of a *white hat hacker*. However, at this point, the ethical and societal issues involved in this have not yet been significantly addressed. This remains a stretch goal for some future time, but these offensive skills are not applicable for public school instruction or activities currently. Teachers, administrators, parents and community members who wish to weigh in on this topic may do so by contacting the appropriate member of their district staff, or the Department of Education and Early Childhood Development (currently Graham Rich, graham.rich@gnb.ca).

3.4 Curriculum Organizers and Outcomes

Organizers

Cybersecurity 120 curriculum has been developed with digital literacy in mind, including inquiry, problem solving and decision making. Inquiry also involves empathy and understanding the challenges that humans are facing. Problem solving involves understanding the human challenges and brainstorming solutions based on a thorough understanding of the people facing the challenge and their expectations for any solution. Decision making involves both solution selection, project management, project testing and quality assurance, as well as evaluation. Decision making also involves selecting a development model (waterfall or agile) and understanding the advantages, disadvantages and consequences over the full lifespan of the project, and over the lifespan of professional projects that they may undertake later if they choose a career involving cybersecurity.

Outcomes

The New Brunswick Curriculum is stated in terms of general curriculum outcomes, specific curriculum outcomes, and achievement indicators.

General Curriculum Outcomes (GCO) are overarching statements about what students are expected to learn in each strand/sub-strand. The general curriculum outcome for each strand/sub-strand is the same throughout the grades.

Specific Curriculum Outcomes (SCO) are statements that identify specific concepts and related skills underpinned by the understanding and knowledge attained by students as required for a given grade.

Learning Outcomes Summary Chart

GCO 1	**Students will demonstrate operational skills specific to supporting and securing digital technology.**
SCO 1.1	Students will persevere and demonstrate resourcefulness when challenges arise during a project.
SCO 1.2	Students will articulate challenges and hypothesize solutions to complete projects and resolve cybersecurity events.
SCO 1.3	Students will use team-based project management strategies during collaborative efforts.
SCO 1.4	Students will apply the fundamentals of digital technology in relation to cybersecurity.

GCO 2	**Students will use computational thinking skills to analyze challenges and to create and evaluate solutions.**
SCO 2.1	Students will decompose a larger challenge into smaller manageable challenges.
SCO 2.2	Students will create repeatable solutions to manageable challenges.
SCO 2.3	Students will represent, collect, organize, and manage data for support and security of digital technologies.
SCO 2.4	Students will analyze data, identify risks, and troubleshoot by using algorithms.
SCO 2.5	Students will execute a solution and evaluate the solution’s validity, efficiency, and effectiveness.

GCO 3	**Students will analyze cybersecurity challenges related to individuals, governments, non-profits, and businesses.**
SCO 3.1	Students will develop an awareness of the current threats, trends, and careers in cybersecurity.
SCO 3.2	Students will analyze preventative and defensive responses—including digital forensics and vulnerability management—to cybersecurity threats.
SCO 3.3	Students will investigate physical, social, and digital practices of safeguarding data, systems, and devices.
SCO 3.4	Students will evaluate the risk and impact that cybersecurity has on privacy.
SCO 3.5	Students will analyze the ethical practices and societal implications related to preventing and responding to cybersecurity threats.

4. Curriculum Outcomes

GCO 1	**Students will demonstrate operational skills specific to supporting and securing digital technology.**
SCO 1.1	**Students will persevere and demonstrate resourcefulness when challenges arise during a project.**

Concepts and Content	**I Can – exemplars:**
Resourcefulness • in the face of challenges, problems, errors and misleading information • to brainstorm, research and discuss possible causes and potential solutions Perseverance • in the face of complex, ambiguous, non-trivial, and difficult-to-grasp challenges • to keep focus on the immediate task and on the larger goal • to keep working and not back down, even if the task is more difficult than ever seen before • to stay working on a task until it is solved or completed	I can be resourceful when brainstorming, researching, analyzing and discussing possible causes and potential solutions to challenges, problems, errors and misleading information. I can analyze, evaluate and continue to be resourceful in the face of ongoing challenges. I can persevere in my work that is complex, ambiguous, non-trivial or difficult to grasp. I can stay focused on a task with multiple potential solutions, and keep in mind both the task and the larger goal. I can keep working on a task, even though it is more difficult than any I've seen before. I can work on a project with complex tasks, whether alone or in a group and I can see the project through to completion.

Resources		
Video	**Website**	**Document**
	https://nbed.sharepoint.com/sites/Cybersecurity120	

SCO 1.2	Students will articulate challenges and hypothesize solutions to complete projects and resolve cybersecurity events.

Concepts and Content	I Can – exemplars:
Articulate challenges • that may involve people and/or technology • to analyze where cybersecurity vulnerabilities exist Hypothesize solutions • that may be involved in completing projects and resolving cybersecurity events • to determine possible strategies to mitigate cybersecurity vulnerabilities • to proactively and reactively mitigate cybersecurity risks involving people and technology • by keeping a record of possible solutions for mitigating a variety of cybersecurity risks	I can explain cybersecurity challenges that may involve people, technology or both. I can analyze cybersecurity challenges and vulnerabilities involving people, technology or both. I can be presented with a situation containing a potential vulnerability and suggest a way to resolve the vulnerability. I can identify useful Internet resources for cybersecurity challenges. I can hypothesize solutions based on the brainstorming, researching, analyzing and discussing possible causes and potential solutions to cybersecurity challenges and vulnerabilities. I can identify and implement proactive strategies for mitigating cybersecurity risks and vulnerabilities, including secure password methodology, software patches and updates. I can identify and implement reactive strategies for mitigating cybersecurity risks and vulnerabilities, including: • setting up a basic operating system with appropriate firewalls, antivirus, and user rights; and, • reconnaissance, exploitation, installation, command and control, lateral movement and exfiltration. I can create and maintain a list of possible solutions to mitigate a variety of cybersecurity challenges, risks and vulnerabilities. I can use cybersecurity vocabulary effectively. I can be given materials (e.g., device images, news article) about a current cybersecurity attack and make a hypothesis about: • the type of cybersecurity attack; • what components were involved; • what actions were taken in the attack; • what resulted from the actions taken; and, • what might have caused the attack to end, either temporarily or permanently.

Resources		
Video	**Website**	**Document**
	https://nbed.sharepoint.com/sites/Cybersecurity120	

<table>
<tr><th colspan="2">SCO 1.3 Students will use team-based project management strategies during collaborative efforts.</th></tr>
<tr><th>Concepts and Content</th><th>I Can – exemplars:</th></tr>
<tr><td>Collaborate
communicate effectively within a team
collaborate online and in-person on team-based tasks
Project Management
identify the roles in effective teams
identify project management strategies
adopt and adapt roles and strategies for a specific group with a specific task
delegate tasks—and receive delegated tasks—that enable a successful cybersecurity project</td><td>I can communicate effectively with my team, and when there is confusion, I can determine how best to improve my communication.

I can communicate and collaborate effectively with my team, both online and in-person.

I can adapt a team management strategy to a specific task and group (e.g., waterfall, agile).

I can be part of a team that delegates tasks with timelines, and I can be accountable for my tasks.

I can share an idea clearly and objectively with my team members.

I can accept comments and criticism about my contributions and suggestions, as our team develops solutions and work plans.

I can identify key roles on effective teams, and I can evaluate the effectiveness of my role on my team.</td></tr>
<tr><th colspan="2">Resources</th></tr>
<tr><th>Video</th><th>Website</th><th>Document</th></tr>
<tr><td></td><td>https://nbed.sharepoint.com/sites/Cybersecurity120</td><td></td></tr>
</table>

SCO 1.4	Students will apply the fundamentals of digital technology in relation to technical support and cybersecurity.

Concepts and Content	I Can – exemplars:

Fundamentals
• to examine and explain the functions of computer hardware and software, and how they work together.
• to examine and explain networking principles, including the design of:
  ○ Local Area Networks (LAN),
  ○ the Internet and
  ○ the World Wide Web (WWW)
• to identify and defend against a variety of threats and vulnerabilities
• to identify the steps involved in a cybersecurity attack
• to examine, explain and implement authentication and access control
• to examine, explain and implement encryption
• to examine, explain and implement intrusion detection
• to identify and defend against a variety of malware
• to explain botnets and their uses and to implement defenses for individuals and businesses
	I can explain how computer hardware functions.
	I can explain how computer software functions, and how it works together with hardware.
	I can identify an unplugged piece of hardware and know where it needs to be plugged in.
	I can identify a hardware issue and a software issue and explain some common differences.
	I can physically identify basic network hardware components such as routers, switches, Ethernet adapters, and wireless adapters.
	I can explain network principles and designs, including LAN, WWW and the Internet.
	I can secure devices – including mobile devices – that use a variety of operating systems.
	I can secure devices by creating, modifying and deleting appropriate user account types and access.
	I can identify steps in a cybersecurity attack and describe how to mitigate against these.
	I can implement authentication and access control.
	I can implement encryption.
	I can implement intrusion detection.
	I can defend against a variety of malware.
	I can explain a botnet and can mitigate against them.
	I can determine if a group of computers is connected to the Internet.
	I can determine if a computer's keyboard, mouse and video displays are working correctly.

Resources

Video	Website	Document
	https://nbed.sharepoint.com/sites/Cybersecurity120	Have You Been Hacked Yet? Stakhanova and Stakhanov (2017)

GCO 2 Students will use computational thinking skills to analyze challenges and to create and evaluate solutions.

SCO 2.1	Students will decompose a larger challenge into smaller manageable challenges.
Concepts and Content	**I Can – exemplars:**
Decompose • in the face of complex, ambiguous, non-trivial and difficult-to-grasp challenges • to analyze and determine why and how complex problems, challenges or tasks can be broken into smaller challenges that can each be solved in turn • to be able to combine solutions to smaller challenges in order to solve the original larger challenge	I can work with complex, ambiguous, non-trivial and difficult challenges. I can decompose a large complex challenge into smaller challenges that are more manageable and more easily solvable. I can combine the solutions to smaller challenges in a way that solves the original larger challenge. I can explain how decomposition is a useful technique in a variety of situations, beyond computers, networks, and cybersecurity.

Resources		
Video	**Website**	**Document**
	https://nbed.sharepoint.com/sites/Cybersecurity120	Have You Been Hacked Yet? Stakhanova and Stakhanov (2017)

<table>
<tr><th colspan="2">SCO 2.2 | Students will create repeatable solutions to manageable challenges.</th></tr>
<tr><th>Concepts and Content</th><th>I Can – exemplars:</th></tr>
<tr><td>Algorithmic Thinking
to clearly define the steps, sequences and rules of a solution to a challenge
to assess a group of problems for similarities (elements in common)
to consider challenges where common elements are being solved repeatedly and, therefore, a common solution can be used
Pattern Recognition and Automation
to recognize situations and challenges where an automated solution can be applied
to recognize the sequences and rules involved in creating a repeatable solution (which may involve human and/or technology automation)</td><td>I can clearly define the steps to solve a challenge.

I can create a solution based on the defined steps.

I can assess groups of challenges for similarities, so that I can create common solutions (which may include loops, policies or other repeatable solutions).

I can secure a variety of digital devices using common patterns and solutions, and I can document the steps in these solutions.

I can guide a peer through the process of securing a digital device, including searching for vulnerabilities.

I can adapt a solution to solve a challenge that has common elements but is slightly different (and may involve human and/or technology automation).

I can use and adapt an existing open source resources to solve a challenge.</td></tr>
<tr><th colspan="2">Resources</th></tr>
<tr><td colspan="2"><table>
<tr><th>Video</th><th>Website</th><th>Document</th></tr>
<tr><td></td><td>https://nbed.sharepoint.com/sites/Cybersecurity120</td><td>Have You Been Hacked Yet? Stakhanova and Stakhanov (2017)</td></tr>
</table></td></tr>
</table>

SCO 2.3	**Students will represent, collect, organize, and manage data for support and security of digital technologies.**
Concepts and Content	**I Can – exemplars:**
Data Representation • to gather data related to cybersecurity events • to use algorithms to generate and present data visualizations • to interpret data (using visualizations) to explain and/or prove a cybersecurity event or challenge	I can gather data related to a cybersecurity event and I can analyze that data to determine important elements. I can use algorithms to help me analyze data from a cybersecurity event, including data visualizations. I can prove, using data, that a cybersecurity event happened. I can explain, using data, how a cybersecurity event happened. I can mitigate a cybersecurity risk and I can use data to prove the mitigation is enabled and effective. I can stay up-to-date on different methods and approaches to fixing cybersecurity issues.

Resources		
Video	**Website**	**Document**
	https://nbed.sharepoint.com/sites/Cybersecurity120	Have You Been Hacked Yet? Stakhanova and Stakhanov (2017)

SCO 2.4	**Students will analyze data, identify risks, and troubleshoot by using algorithms.**
Concepts and Content	**I Can – exemplars:**
Algorithmic Thinking • to evaluate and defend a cybersecurity target by analyzing data, and by identifying and mitigating risks • to create a repeatable list that will help investigate and solve issues related to cybersecurity events • to explain how algorithms are used by online systems, and the potential inaccuracies and vulnerabilities Analysis • to troubleshoot a cybersecurity event, including vulnerability management • to design a troubleshooting guide to help others respond to cybersecurity events • to evaluate and improve a troubleshooting guide	I can defend a cybersecurity target by analyzing data and mitigating risks. I can create a list of issues to check with each cybersecurity event. I can explain how algorithms might have inaccuracies and vulnerabilities when used by online systems. I can troubleshoot a cybersecurity event using a variety of tools including vulnerability management. I can design a troubleshooting guide, including the above elements, to help others respond to cybersecurity events. I can evaluate and improve troubleshooting guides created by me and by others. I can analyze potential vulnerabilities using available networking tools. I can discover flaws and security threats on digital devices.

Resources		
Video	**Website**	**Document**
	https://nbed.sharepoint.com/sites/Cybersecurity120	Have You Been Hacked Yet? Stakhanova and Stakhanov (2017)

<table>
<tr><th colspan="3">SCO 2.5 | Students will execute a solution and evaluate the solution's validity, efficiency, and effectiveness.</th></tr>
<tr><th>Concepts and Content</th><th colspan="2">I Can – exemplars:</th></tr>
<tr><td>Execute a Solution
to finalize and complete a solution to a cybersecurity problem or challenge
to implement, execute, and engage a solution to a cybersecurity problem or challenge
Evaluate a Solution
to evaluate, test, or validate a solution to a cybersecurity problem or challenge
to assess or appraise a solutions efficiency and effectiveness regarding a cybersecurity problem or challenge</td><td colspan="2">I can complete a solution to a cybersecurity challenge.

I can implement and execute my solution to a cybersecurity challenge.

I can evaluate, test, or validate a cybersecurity challenge's solution (that is either an existing resource or was made by me or my group).

I can assess or appraise the efficiency and effectiveness of a solution to a cybersecurity challenge's solution, whether it was created by me or not.</td></tr>
<tr><th colspan="3">Resources</th></tr>
<tr><th>Video</th><th>Website</th><th>Document</th></tr>
<tr><td></td><td>https://nbed.sharepoint.com/sites/Cybersecurity120</td><td>Have You Been Hacked Yet? Stakhanova and Stakhanov (2017)</td></tr>
</table>

GCO 3 Students will analyze cybersecurity challenges related to individuals, governments, non-profits, and businesses.

SCO 3.1 Students will develop an awareness of the current threats, trends, and careers in cybersecurity.

Concepts and Content	I Can – exemplars:
Threats • to appraise or assess threat agents (natural, human, and technical) • to defend or mitigate multiple types of vulnerabilities involving natural, human, physical, media, hardware, or software • to identify the stages and lifecycle of a cybersecurity attack Trends • to research and identify current trends in cybersecurity attacks and events • to identify the common types of people who are hackers. • to identify the classifications of hackers Careers • to identify and investigate cybersecurity career options and pathways	I can list potential cybersecurity threat agents (natural, human, and technical). I can appraise or assess cybersecurity threat agents. I can defend multiple types of vulnerabilities, including natural, human, physical, media, hardware, or software. I can identify the stages (or lifecycle) of a cybersecurity attack. I can determine the usefulness of guides found on the Internet for software and cybersecurity updates. I can research current trends in cybersecurity. I can identify the types of hackers, including script kiddies, semi-skilled hackers, and professionals. I can identify the classifications of hackers, including white hat, grey hat, and black hat. I can identify careers and pathways in cybersecurity, including extra-curricular, post-secondary, internship, and companies involved in cybersecurity in New Brunswick.

Resources

Video	Website	Document
	https://nbed.sharepoint.com/sites/Cybersecurity120	Have You Been Hacked Yet? Stakhanova and Stakhanov (2017)

<table>
<tr><th>SCO 3.2</th><th colspan="2">Students will analyze preventative and defensive responses—including digital forensics and vulnerability management—to cybersecurity threats.</th></tr>
<tr><th colspan="2">Concepts and Content</th><th>I Can – exemplars:</th></tr>
<tr><td colspan="2">Responses:
to identify and perform preventative responses to cybersecurity threats
to identify and perform defensive responses to cybersecurity threats
to perform digital forensics with a variety of operating systems
to perform vulnerability management with a variety of operating systems</td><td>I can perform preventative responses to cybersecurity threats, including:
I can install anti-virus software.
I can setup a default firewall.
I can setup user and guest accounts with appropriate access.
I can setup administrator accounts with appropriate access.
I can secure a computer image of a Windows Operating System (OS) so that it is a reasonably safe setup for basic network and Internet use.
I can secure a computer image of a Linux OS that it is a reasonably safe setup for basic network and Internet use.
I can identify a variety of specific defensive responses, including:
those found within digital forensics and vulnerability management, and
those found in desktops, laptops and mobile devices.
I can perform digital forensics in a Windows OS image and in a Linux OS image.

I can understand that there is no one single cause of a cybersecurity event.

I can perform vulnerability management in a Windows OS image and in a Linux OS image.

I can investigate aspects of cybersecurity events on mobile devices (e.g., smartphones, tablets).</td></tr>
<tr><th colspan="3">Resources</th></tr>
<tr><th>Video</th><th>Website</th><th>Document</th></tr>
<tr><td></td><td>https://nbed.sharepoint.com/sites/Cybersecurity120</td><td>Have You Been Hacked Yet? Stakhanova and Stakhanov (2017)</td></tr>
</table>

SCO 3.3	Students will investigate physical, social, and digital practices of safeguarding data, systems, and devices.
Concepts and Content	**I Can – exemplars:**
Safeguarding: • to recognize the purposes and principles for safeguarding data, systems, and devices • to evaluate effective safeguarding practices • to perform safeguarding practices with data, systems, and devices • to debate and make supporting arguments regarding principles of confidentiality, system availability, and data integrity • to determine and enact countermeasures to a threat that may involve natural, human, physical, media, hardware, or software elements • to understand and enact access control through identification, authentication, and authorization • to understand the nature of password attacks and to evaluate policies designed to prevent these attacks • to differentiate between types of encryption, including symmetric and asymmetric • to differentiate between types of asymmetric encryption, including public and private keys	I can list the principles for safeguarding data, systems and devices. I can evaluate safeguarding practices for effectiveness. I can perform safeguarding practices with data, systems and devices. I can list and support the principles of confidentiality, system availability and data integrity. I can enact countermeasures to a cybersecurity threat that may involve natural, human, physical, media, hardware, or software elements. I can enact access control through the processes of identification, authentication, and authorization. I can evaluate policies designed to prevent password attacks. I can explain the differences between symmetric and asymmetric encryption. I can use asymmetric encryption involving public and private keys. I can configure system security policies. I can develop methods of secure password use. I can explain and demonstrate multi-factor authentication using networked platforms.
Resources	
Video	**Website** https://nbed.sharepoint.com/sites/Cybersecurity120 **Document** Have You Been Hacked Yet? Stakhanova and Stakhanov (2017)

SCO 3.4 | **Students will evaluate the risk and impact that cybersecurity has on privacy.**	
Concepts and Content	**I Can – exemplars:**

Privacy
• to recognize the importance of the privacy of personal information
• to evaluate systems for their protection and privacy of personal information
• to evaluate systems for the access and control provided to users regarding their privacy and personal information
• to evaluate data breaches and their impact on data, systems, and devices
• to evaluate data breaches and the damage to individuals and organizations including repercussions that involve:
  ○ financial loss and loss of revenue,
  ○ compensation claims,
  ○ psychological distress,
  ○ emotional distress, and
  ○ loss of reputation and trust.
	I can recognize the importance of the privacy of personal information, including informing the individual of:
	• storage and use of their personal information, and
	• data breaches of their personal information.
	
	I can evaluate human and technological systems for their protection and privacy of personal information, including the stated and actual uses of personal data as described in policies.
	
	I can evaluate human and technological systems for the access and control provided to users regarding their privacy and personal information.
	
	I can evaluate data breaches and their impact on data, systems and devices.
	
	I can evaluate data breaches and their damage to individuals and organizations, including:
	• financial loss and loss of revenue,
	• individual or business compensation claims,
	• psychological and emotional distress,
	• loss of the company's reputation, and
	• loss of customer's trust.
	
	I can evaluate the extent of personal information revealed when a victim responds to a phishing communication, by email, text, or some other way.
	
	I can identify the loss of privacy and personal data if someone were to use my username and password.

	I can choose my preferred level of privacy, and I can set the level of privacy offered by a social media service (site or app). I can define and describe a digital footprint, including: • its main components, • why it is important to be cautious and intentional about what information I share publicly or on social media, • why it is important to know what information others are sharing about me, including friendly tagging and unfriendly bullying, and • why it is important to know what information an online service is sharing about me.

Resources

Video	Website	Document
	https://nbed.sharepoint.com/sites/Cybersecurity120	Have You Been Hacked Yet? Stakhanova and Stakhanov (2017)

SCO 3.5	Students will analyze the ethical practices and societal implications related to preventing and responding to cybersecurity threats.
Concepts and Content	**I Can – exemplars:**
Ethical Practices: • to identify ethical implications of a cybersecurity situation or case Social Implications: • to distinguish between cybersecurity events that are ethical and unethical, legal, and illegal • to recognize and evaluate Canadian laws designed to protect individuals and organizations regarding cybersecurity events	I can identify ethical implications, for an individual or for a group – of a cybersecurity situation or case. I can distinguish ethical and unethical cybersecurity situations, cases or events. I can differentiate between ethical (white hat) and unethical (black hat) hacking. I can distinguish legal and illegal cybersecurity situations, cases or events. I can evaluate Canadian laws about cybersecurity involving individuals and organizations. I can identify the main points and social implications in a news article about a cybersecurity issue.

Resources		
Video	**Website** https://nbed.sharepoint.com/sites/Cybersecurity120	**Document** Have You Been Hacked Yet? Stakhanova and Stakhanov (2017)

5. Bibliography

Common Content

Universal Design for Learning, Center for Applied Special Technology (CAST) http://www.cast.org/

Nelson, Louis Lord (2014). Design and Deliver: Planning and Teaching Using Universal Design for Learning. 1st Edition, Paul H. Brooks Publishing Co.

Teacher Resources

Kaplan, F. M. (2017). *Dark territory: the secret history of cyber war*. New York: Simon & Schuster Paperbacks.

Stakhanova, N., & Stakhanov, O. (2017). *Have you been hacked yet?: how to protect your personal and financial information today*. Victoria, B.C.: Tellwell Talent.

6. Appendices

6.1 New Brunswick Global Competencies

Critical Thinking and Problem-Solving	Innovation, Creativity, and Entrepreneurship	Self-Awareness and Self-Management
• Engages in an inquiry process to solve problems • Acquires, processes, interprets, synthesizes, and critically analyzes information to make informed decisions (i.e., critical and digital literacy) • Selects strategies, resources, and tools to support their learning, thinking, and problem-solving • Evaluates the effectiveness of their choices • Sees patterns, makes connections, and transfers their learning from one situation to another, including real-world applications • Analyzes the functions and interconnections of social, ecological, and economic systems • Constructs, relates and applies knowledge to all domains of life, such as school, home, work, friends, and community • Solves meaningful, real-life, and complex problems by taking concrete steps to address issues and design and manage projects • Formulates and expresses questions to further their understanding, thinking, and problem-solving	• Displays curiosity, identifies opportunities for improvement and learning, and believes in their ability to improve • Views errors as part of the improvement process • Formulates and expresses insightful questions and opinions to generate novel ideas • Turns ideas into value for others by enhancing ideas or products to provide new-to-the-world or improved solutions to complex social, ecological, and economic problems or to meet a need in a community • Takes risks in their thinking and creating • Discovers through inquiry research, hypothesizing, and experimenting with new strategies or techniques • Seeks and makes use of feedback to clarify understanding, ideas, and products • Enhances concepts, ideas, or products through a creative process	• Has self-efficacy, sees themselves as learners, and believes that they can make life better for themselves and others • Develops a positive identity, sense of self, and purpose from their personal and cultural qualities • Develops and identifies personal, educational, and career goals, opportunities, and pathways • Monitors their progress • Perseveres to overcome challenges • Adapts to change and is resilient in adverse situations • Aware of, manages, and expresses their emotions, thoughts, and actions in order to understand themselves and others • Manages their holistic well-being (e.g., mental, physical, and spiritual) • Accurately self-assesses their current level of understanding or proficiency • Advocates for support based on their strengths, needs, and how they learn best • Manages their time, environment, and attention, including their focus, concentration, and engagement

Collaboration	Communication	Sustainability and Global Citizenship
• Participates in teams by establishing positive and respectful relationships, developing trust, and acting interdependently and with integrity • Learns from and contributes to the learning of others by co-constructing knowledge, meaning, and content • Assumes various roles on the team and respects a diversity of perspectives • Addresses disagreements and manages conflict in a sensitive and constructive manner • Networks with a variety of communities/groups • Appropriately uses an array of technology to work with others • Fosters social well-being, inclusivity, and belonging for themselves and others by creating and maintaining positive relationships with diverse groups of people • Demonstrates empathy for others in a variety of contexts	• Expresses themselves using the appropriate communication tools for the intended audience • Creates a positive digital identity • Communicates effectively in French and/or English and/or Mi'kmaq or Wolastoqey through a variety of media and in a variety of contexts • Gains knowledge about a variety of languages beyond their first and additional languages • Recognizes the strong connection between language and ways of knowing the world • Asks effective questions to create a shared communication culture, attend to understand all points of view, express their own opinions, and advocate for ideas	• Understands the interconnectedness of social, ecological, and economic forces, and how they affect individuals, societies, and countries • Recognizes discrimination and promotes principles of equity, human rights, and democratic participation • Understands Indigenous worldviews, traditions, values, customs, and knowledge • Learns from and with diverse people, develop cross-cultural understanding • Understands the forces that affect individuals and societies • Takes action and makes responsible decisions that support social settings, natural environments, and quality of life for all, now and in the future • Contributes to society and to the culture of local, national, global, and virtual communities in a responsible, inclusive, accountable, sustainable, and ethical manner • Participates in networks in a safe and socially responsible manner.
Foundation of Literacy and Numeracy		

6.2 Universal Design for Learning (UDL)

UDL helps meet the challenge of diversity by suggesting flexible instructional materials, techniques, and strategies that empower educators to meet these varied needs. UDL research demonstrates that the challenge of diversity can and must be met by making curriculum flexible and responsive to learner differences. UDL provides guidelines to minimize barriers and maximize learning for all.

Is there a form of **assistive technology** that could be used to enhance/facilitate this lesson?	Screen readers, screen magnifiers
Are there **materials which can appropriately challenge** readers to enhance this learning?	The online teacher resource site as well as the Cyber Defense Hub (using the NetLab+ system) contains online lessons (PDF documents) and virtual machines useful for demonstrating learning.
Are there students in this group who cannot **access this learning (PLP background)** and whose needs I must revisit before teaching?	View previous PLP information for considerations
Are there other **choices** that can be provided in this learning opportunity?	Learning can be differentiated for outcomes as well as for depths of learning and methods of demonstrating learning.
Is there another/a **variety of media** available? Only paper-based? Can it be listening? Can I add a visual component?	The online teacher resource site as well as the Cyber Defense Hub provides all lessons online and these can be printed.
Can **movement** be involved?	Students can perform this learning on any device, although the virtual machines (Cyber Defense Hub) work best on a full monitor.
Grouping and regrouping?	Learning can be cooperative and in teams. Learning can be demonstrated using virtual machines and in games and competitions.
Teacher versus non teacher centered? **Instructional design strategies**	Learning always revolves around the teacher, but opportunities exist for students to be more self-directed and self-paced using online resources and project-based learning. Students can self-initiate projects.
Opportunities for students to **propose variations** to the assignments/projects?	The initial tutorials are very straightforward and pre-set. However, once students demonstrate learning the fundamentals, then there are many opportunities for student project variation.
Use of **art /music / technology**?	Almost all student resources for this course are available online. There are many additional online resources, including web sites and YouTube videos.
Can I use **drama**?	Role playing and artistic expression can be used in many ways to explain or demonstrate learning about cybersecurity topics including ethical, psychological, sociological and philosophical elements.
Is there a plan to support the student/s who might already know this subject matter? **Enrichment**	Students can prove prior learning and have opportunities to advance and enrich their own learning. This can be through self-paced tutorials or through self-initiated project proposals.

Does the **language level** need to be adjusted for the student to access this learning?	This course is very dependent on the use of the English language. While students can use online translators for context, the demonstrations of learning using virtual machines must be done in English as the underlying computer systems are all written in English. (This is the reality of all computer systems around the world.)
Is there an **independent** or **collaborative activity-project** that would be better meet the needs of one or more students?	This course is largely based on tutorial work that leads to project-based learning. This work can be done independently or collaboratively, based on the needs of the student.
Are there any **experts** that I could bring into the classroom electronically or as a guest speaker?	There are many speakers available, locally and online, as well as documentary videos and local labour market data.
Have I linked the goal to as current event or a cultural event in the student's lives? Can I make the learning more **relevant**?	Cybersecurity is a topic that is relevant to every person on earth. This course starts slowly and builds quickly to cover a wide array of topics under the cybersecurity heading. Almost any activity or topic can now have a cybersecurity element to it, so there's no limits here.
Is there a **hands-on experience** that we could do to launch this lesson or this learning?	The learning is usually demonstrated through hands-on configuration of virtual machines in a safe online environment.

7. Teacher Resources

Approaches to Teaching

Cybersecurity 120 teachers are encouraged to evolve from the lecture format to that of a guide, a coach, and a mentor. The Cybersecurity 120 curriculum is designed with project-based learning in mind.

A fundamental principle of this course is that students assume responsibility for their own learning (ownership) through an inquiry-based/project-based learning approach. Since these strategies may be new to many students, teachers should discuss methods of organizing and brainstorming the big questions for inquiry and introduce resources that help students critically address problems.

Students will know, and be able to use, strategies and processes to think creatively, understand deeply, conduct meaningful reflection, and solve problems independently and collaboratively. Students should be continuously aware of and planning for physical security and cybersecurity while applying Global Competencies.

Being exposed to programs that involve collaboration and communication will develop important competencies mentioned above. Students should be encouraged to be resourceful and search the myriad of open source resources available on the internet to assist them in solving open ended problems. Having students provide documentation within their problem solving, as well as in the design, will help students to understanding the meaning of functions, services, policies and processes of cybersecurity.

Software Selection

A variety of software is available for use in Cybersecurity 120. The Department of Education and Early Childhood Development (EECD) is currently working with partners, both local and global, to provide safe yet practical cybersecurity environments for our students. EECD wishes to thank those partners, as well as our technical staff including those in-house, in the districts and in schools. As these partnerships are currently being established, persons who wish to find out more information can contact EECD staff directly. At the time of publication, that person is Graham Rich (graham.rich@gnb.ca) Information and Communication Technology Learning Specialist.

Sample Course Timetable

Timeline	Focus
Day 1	Focus on hands-on activities on day one: the more engaging, the better!
Weeks 1-3	Introduction to basic computer and network functions, with eye to cybersecurity risks.
End of Week 3	Students will have produced at least one artifact (used in summative assessment).
Weeks 4-6	Introduction to the current and historic variety of cybersecurity vulnerabilities.
End of Week 6	Students will have produced an artifact based on a project-based approach.
Weeks 7-9	Introduction to preparing and defending computer environments.
End of Week 9	Students will have begun a project to produce an artifact, likely a virtual image.
Weeks 10-13	Students will understand the size and scope of cybersecurity threats and mitigations.
End of Week 13	Students will have completed a project to produce an artifact, likely a virtual image.
Weeks 14-19	Mastery of fundamentals and/or extension into advanced cybersecurity topics.
End of Week 19	Students will produce a capstone project.