A Cyber Range In Education

Alternative And Modern Cybersecurity Education Approaches Are Needed To Solve The Increasing Cybersecurity Talent Gap In Canada

ENFOCOM CYBERSECURITY

LEARN MORE AT ENFOCOM.COM

White Paper

Problem

Increasing Cybersecurity Talent Gap In Canada And Worldwide

Situation

Cybersecurity education has gotten little to no attention in higher education institutions

Solutions

Alternative and modern cybersecurity education approaches are needed

Technology

Cyber Ranges have emerged as interactive, simulated platforms with representations of networks, systems, tools, and applications to provide safe, legal environments to gain hands-on cyber skills and a secure environment for product development and security-posture testing

LEARN MORE AT ENFOCOM.COM

The Problem

Increasing Cybersecurity Talent Gap In Canada And Worldwide

Cybersecurity has long been recognized as the responsibility of the whole enterprise and not simply the IT department. The previous year (2022) has only highlighted that fact, with over 4,000 attacks of only ransomware[1] occurring daily. On average, these attacks result in 16 days of system outages,[2] 92% of companies who paid ransomware not only did not get all their data back[3] but also, in 80% of cases, experienced another attack,[4] and 104% increase in average ransomware payment amount from 2019.[5] These numbers become even worse as we move to Advanced Persistent Threats (APT); because of their specific methods used, it can take an average of 240 days to detect APT-related breaches.[6] What is most critical in all these statistics, however, is the fact that across the companies that weren't hit by the ransomware, the number one reason was the presence of trained staff within the organization, and while the focus of the report was on the IT staff, it is becoming clear that the security posture of the organization is in the hands of all the staff.[7]

The above-described situation is worsened by an increasing cybersecurity talent gap in Canada and worldwide.[8] Specifically, the Information and Communications Technology Council (ICTC) reports that one in six cybersecurity jobs go unfilled.[9] The ICTC's report also identified a clear communication gap between the industry and academia, as the employers and students had different views and understanding of the Canadian cybersecurity job market landscape.[10] Moreover, The (ISC)² Cybersecurity Workforce Study report, published in 2022, identified a global cybersecurity workforce gap of 3.4 million people, with approximately 436,000 positions in North America and 25,000 in Canada. Despite the addition of over 464,000 workers in the past year, the cybersecurity workforce gap has grown more than twice as much as the workforce, indicating a supply that lags behind the growing demand.[11] All of the above outlines a clear need for alternative education methods and pathways in the cybersecurity field.

Traditional Approach to Cybersecurity Education

Doesn't Cover Real-world Scenarios

Traditionally, cybersecurity has gotten little to no attention in higher education institutions, with a survey done in 2016 showing that none of the top 10 US universities required students to take a cybersecurity class, and three of the top 10 didn't offer any cybersecurity courses at all.[12] Even when the courses were being taught the traditional approach was to often start by covering abstract concepts that don't directly apply to the real-world scenarios, and rarely give the students a chance to test out the concepts in a hands-on way. With IBM highlighting the fact that cybersecurity positions take 20% longer to fill when compared to other typical IT-related positions[13] and a survey done by McAfee revealing that only 23% of employers believe that education programs are preparing students sufficiently to enter the cybersecurity industry, it is no surprise if a new hire would need to go through a lengthy and rigorous training process before starting their core responsibilities. This situation is not ideal for organizations that are already struggling to tackle an ever-growing cyber threat landscape while highly understaffed, as experienced and knowledgeable cybersecurity professionals become overwhelmed and exhausted and choose to leave the industry.[14] Consequently, emerging alternative cybersecurity education methods and pathways are being tested to not only introduce new influx of cybersecurity specialists into the field but also increase the level of practical and real-world skillsets that the new hires possess.

Alternative Cybersecurity Education Pathways

Experiential Learning Theory (ELT)

A substantial component that leads to the success of any educational program is vocational training. Traditionally, many institutions have provided practical and hands-on training for workers to develop the skills necessary to succeed. Providing students with the opportunity to work with technologies, platforms and assets currently offered in the industry is a key component of this type of training. Many types of vocational training are provided to learners across various disciplines, e.g., internships, situated learning and apprenticeships, which recently have been combined under the Experiential Learning Theory or ELT.

ELT was developed by David A. Kolb, an American educational theorist and psychologist. He first introduced the theory in the 1970s and expanded upon it in subsequent years.[15] The theory is commonly defined in two levels: a four-stage learning cycle and four different learning styles. The learning cycle is based on the idea that the learner "touches all the bases," specifically:[16]

1. The learner **encounters a concrete experience**. This might be a new experience or situation or a reinterpretation of existing experience in the light of new concepts.
2. The learner **reflects on the new experience in the light of their existing knowledge**. Of particular importance are any inconsistencies between experience and understanding.
3. The learner **forms an abstract conceptualization**. The previous reflection gives rise to a new idea or a modification of an existing abstract concept (the person has learned from their experience).
4. The learner **begins active experimentation**. The newly created or modified concepts give rise to experimentation. The learner applies their idea(s) to the world around them to see what happens.

Four Major Types Of Learning Styles

The high-level idea behind the learning cycle is that each subsequent step allows learners to form increasingly complex and abstract “mental models” of the learning material and topic.

In addition to recognizing the importance of the learner's steps during different learning stages, Kolb also recognized that different people naturally lean towards certain learning styles. He was able to group them into four major types:

1. Concrete Experience (CE) - Learners with this learning style prefer direct experiences and engage with the actual materials or situations. They rely on personal involvement and sensory experiences to grasp new concepts.
2. Reflective Observation (RO) - Learners with this learning style prefer to observe and reflect upon their experiences. They carefully consider the situation, analyze it from different perspectives, and often take a more thoughtful and introspective approach to learning.
3. Abstract Conceptualization (AC) - This learning style involves forming theories, concepts, and models to understand information. Learners with this style prefer to think abstractly and engage in logical and analytical reasoning. They focus on creating conceptual frameworks to make sense of their experiences.
4. Active Experimentation (AE) - Learners with this learning style enjoy actively applying their learning and testing theories in practice. They prefer hands-on experiences, trial and error, and practical application. They are willing to take risks and learn through action.

Common Pathways For Building A Career In Cybersecurity

Combining the various learning cycles with different learning styles led to the development multiple pathways for building careers in different disciplines, including cybersecurity. These pathways allow learners to pursue a cybersecurity career based on their learning styles, circumstances, career aspirations and other factors. Below we describe at a high level some of the common pathways for building a career in cybersecurity:[17]

- **Academic Pathway** – This would be viewed as a traditional approach to building a career in cybersecurity that includes the consecutive completion of formalized educational programs with individuals alternating or combining studies with work. The specific paths vary between the individuals. For example, someone may enroll in a community college program, while someone else may pursue a graduate school, so this pathway may not be as straightforward as may be viewed in the beginning.
- **Cooperative Education** – In this pathway, a student enrolls in a higher education institution with an arrangement with employers. In this case, learners are students first and employees second, in reality, there will be times when a learner has an alternating relationship between academic studies and work.
- **Apprenticeship** - An increasingly popular pathway in which employers establish apprenticeship programs. In this pathway, the learners are employees first and students second. The benefit of cooperative education and this pathway is that the learners can "Earn as they learn" and obtain the additional benefit of employer-supported education and training.
- **Reskilling** – This pathway is focused on working adults who may also pursue a cybersecurity career even if they have not previously acquired cybersecurity credentials or related work experience. Reskilling or upskilling typically includes participation in an academic or training program that facilitates a career change. This pathway is particularly attractive to individuals who are unemployed, underemployed or are transitioning from other careers.

Remote Learning And Flexibility Have Become Increasingly Prevalent

In addition to the diverse pathways mentioned above, remote learning and flexibility have become increasingly prevalent in the field of education.

Remote learning has emerged as a game-changer, enabling individuals to access educational programs and training from anywhere in the world. With advancements in technology, remote learning is becoming more interactive and immersive than ever, offering virtual classrooms, collaborative tools, and hands-on practical exercises.

Flexibility is another key aspect that has gained importance in the realm of education and training. Many individuals have responsibilities such as jobs, families, or other commitments that may make pursuing a traditional full-time educational program challenging. Flexibility allows learners to balance their professional and personal obligations while still acquiring the necessary skills and knowledge for a cybersecurity career.

The combination of remote learning and flexibility has revolutionized many aspects of the above-mentioned pathways. Through remote learning platforms and flexible programs, many working adults can participate in academic or training courses tailored to facilitate a career change.

In conclusion, the path to a cybersecurity career is as varied as the diverse type of work you are likely to assume, given the changing nature of technology and cybersecurity risks. Various options are available at different levels of cost and time commitment. However, no matter the pathway one chooses or the learner's learning style, there is an increasing number of resources and guidelines that are targeted at enhancing the experience for learners, education and training providers, and employers. Consequently, it is also crucial for learners, education and training providers, and employers to embrace these resources and guidelines.

Modern Cybersecurity Education Approach

The modern approach to cybersecurity education aims to move away from theory-only based programs that provide limited or no practical elements. The goal is also to increase the turnaround time of the new cybersecurity specialists since the current number of specialized graduates doesn't meet the growing demand for cybersecurity specialists. With this in mind, the tools used in modern cybersecurity education address traditional approach limitations by providing collaborative and more experience-oriented programs that allow preparing an interdisciplinary cohort to meet the rising challenges in the cybersecurity landscape. Specifically, several works have suggested utilizing Cyber Ranges with varying capabilities at the core of modern cybersecurity education.[18] ,[19] ,[20] While the specific components of the proposed Cyber Ranges may vary, they still have some common ideas that unite them and allow them to address the challenges mentioned above.

What is Cyber Range?

Cyber Ranges are defined in many ways, with definitions varying depending on the definition's context and goal. For our purposes, we chose the following two definitions:

1. *"Cyber ranges are interactive, simulated platforms and representations of networks, systems, tools, and applications. They typically provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security-posture testing."*[19]

2. *"A cyber range is a controlled, interactive technology environment where up-and-coming cybersecurity professionals can learn how to detect and mitigate cyber-attacks using the same kind of equipment they will have on the job. The range simulates the worst possible attacks on IT infrastructure, networks, software platforms and applications."*[21]

Both of these definitions highlight the fundamental characteristics and purposes of Cyber Ranges. When we explore them, we can notice that they define the goal of Cyber Ranges as providing a realistic and immersive experience for individuals to develop and enhance their cybersecurity capabilities. This simulated nature of Cyber Ranges allows learners to encounter diverse attack scenarios, including known and emerging threats. This exposure helps the learners to understand the intricacies of cyber-attacks and equips them with the necessary skills and knowledge to effectively counteract such threats.

Cyber Range Benefits

Building upon the understanding established by the definitions, we can now explore the advantages that Cyber Ranges offer from the learner's and educator's perspectives.

Learner's Perspective

From the above definitions, it is easy to notice how the Cyber Range moves the focus from theory-based to a hands-on and practical learning experience, where the learners can practice and experience the tools and scenarios presented during the theory parts of the course. The Cyber Range offers learners the ability to experience and practice such skills as:[22]

- **Assessing** the security posture of an enterprise environment and providing recommendations to improve the posture.
- **Monitoring and securing** various environments, including IoT, OT, cloud and mobile.
- **Applying** applicable laws, procedures and policies that include governance, risk and compliance to the environments.
- **Identifying, analyzing, reporting and responding** to security events and incidents.

In addition, it's important to note the collaborative and group aspects of Cyber Ranges. Educators can create scenarios for learners to experience cyber incidents from multiple perspectives. Commonly used scenarios in Cyber Ranges are:[23]

- **Capture the flag** – An event where "flags" are secretly hidden in purposefully-vulnerable programs or websites. In this event, both individuals and teams can participate.
- **Red and Blue team exercises** – In this event, the red team attempts to get into the network, while the opposing blue team attempts to detect, investigate, and respond. As an extension, it is also possible to provide Purple team exercises in which Red and Blue teams work collaboratively to improve the enterprises' security posture.

It's important to note that Cyber Ranges are not restricted to the scenarios mentioned above. Cyber Ranges are highly flexible and adaptable, which means they can be adjusted in close to real-time to support a wide variety of scenarios, reflecting the ever-evolving cybersecurity landscape.

Overall, ENFOCOM's observation from working with higher education institutions is that Cyber Ranges allow for creatively and cognitively involving the learner in ways that traditional approaches do not. This involvement drives motivation, knowledge, and skill retention in the upcoming cybersecurity workforce. Additionally, the adaptability of the Cyber Range to different learning styles and cycles makes it easier for learners to engage with the material in ways that previously were not readily achievable.

Educator's Perspective

Cyber Ranges equally benefit learners and educators. For educators, the Cyber Range offers ease of setup, adaptability, and visibility compared to the previously rigid curricula setup, where sometimes even a minor change to the materials may result in hours of work for the educator and their team. With Cyber Range, educators can:

- Use graphical user interfaces brought up on their browsers to click, drag and drop virtual machines and links between them to set up a scenario and then use it in their classes.
- Save the produced scenarios as a template, adapt them on the fly for the course and benefit of the learners, and re-use them in other teaching or research engagements.
- Get visibility into individual learners' progress and actions by allowing the educator to take the point of view and lead the learner to the desired outcome.
- Assess and evaluate learners' skills and knowledge. Educators can create custom assessments and challenges within the Cyber Range environment to gauge learners' understanding of cybersecurity concepts, identify areas of improvement, and measure their proficiency in different skill areas. This enables educators to provide personalized feedback and support to students, fostering their cybersecurity skills and proficiency growth.

In addition to the above capabilities, the Cyber Ranges commonly come with pre-existing content libraries informed by real-world attack methods and scenarios, allowing educators to integrate the existing content into their curricula and speed up the teaching material development while keeping it current and up-to-date.

Not Every Cyber Range is Fit for Education

Not all of the above capabilities are supported by all the Cyber Ranges, so this naturally leads to the discussion of the differences between the Cyber Ranges. During the initial development of ENFOCOM's Cyber Range, we noticed that the education sector has unique challenges that need to be addressed and are not part of a generic Cyber Range solution. In particular, we observed that the Cyber Range solution for education needs to provide the following:

- **Learning Management System (LMS) Integration** - Integration with a learning management system can enhance educators' and learners' experience by seamlessly integrating Cyber Range activities with the learning ecosystem. The integration enables educators to incorporate Cyber Range exercises and assessments into their course structure, track student progress, and manage grading within the LMS.
- **Gamification and Engagement** - To enhance learners' motivation and engagement, educational Cyber Ranges should incorporate gamification elements. This can include leaderboards, achievements, badges, or rewards to recognize and incentivize learner progress and accomplishments. Gamification encourages healthy competition and helps create a more enjoyable and immersive learning experience.
- **Integration with Various Industry Tools and Technologies** - It is crucial for educational Cyber Ranges to provide integration with various industry-standard tools and technologies used in cybersecurity. This ensures learners gain practical experience with the same tools and techniques used in real-world cybersecurity environments, preparing them for industry roles.
- **Customizability and Flexibility** - Educational Cyber Ranges should allow educators to customize the training environments, exercises, and challenges to align with their curriculum and learning objectives. Flexibility in designing and modifying the Cyber Range content enables educators to adapt the cyber range to evolving cybersecurity trends and address specific educational requirements.

Depending on the purpose of the Cyber Range, some, if not all, of these components may be missing.

On an organizational level, choosing the right Cyber Range solution also requires careful consideration. Institutions want to maximize their investment in terms of educational outcomes and learner success. When selecting a Cyber Range, educational institutions should prioritize features that align with their specific needs. For example, integration with an LMS may be crucial, as it streamlines the learning experience by seamlessly integrating Cyber Range activities with the existing learning ecosystem.

From a teaching and learning point of view, consider a scenario where a Cyber Range is specifically designed to simulate phishing attacks on an enterprise. In this case, the Cyber Range may have pre-defined scenarios and limited content tailored to that particular type of attack. While it provides valuable hands-on experience for phishing incidents, it may not cover other crucial aspects of cybersecurity, such as network intrusion detection. This limitation hinders learners from gaining a comprehensive understanding of the broader cybersecurity field.

As a result, the limitations of Cyber Range can hinder learners from acquiring and practicing essential skills and impede educators from delivering effective instruction. On one side, learners need current learning environments and materials that allow the trial and error necessary to keep pace with the evolving cybersecurity landscape. Furthermore, such Cyber Range capabilities as team-based training are critical to enabling learners to experience the collaboration environment required in the workplace. Conversely, educators who choose Cyber Ranges that lack the above capabilities may miss out on benefits like customized and reusable scenarios, integration with LMS for real-time monitoring of learner performance, and creation of collaborative learning environments.

Conclusion

Cybersecurity Calls For A Modern Approach To Cyber Education

In conclusion, the current cybersecurity landscape calls for a modern approach to cyber education that meets the growing demands for a new cybersecurity workforce, embraces today's learners' online learning styles, engages them through unique game-play storylines, and shifts the learning paradigm to collaborative, dynamic, AI-powered experiences. Cyber range solutions are seen at the core of the new and modern cybersecurity education framework. Having evolved significantly from their military-based origins in 2002, Cyber Ranges help to ensure that the next generation of cyber professionals is well-prepared to combat evolving threats.

Academic institutions have a remarkable opportunity to lead the way in progressive, next-generation learning approaches that utilize Cyber Ranges to equip learners for the dynamic workplace in cybersecurity. A high-fidelity, cloud-secure Cyber Range can address the challenges faced in traditional cybersecurity education approaches and provide learners with invaluable opportunities to acquire practical skills and knowledge.

By integrating key features such as LMS integration, gamification, industry tool integration, and customizability, educational Cyber Ranges can effectively support the development of the next generation of cybersecurity professionals. Ongoing collaboration between educators, industry professionals, and cybersecurity experts, coupled with continuous advancements in Cyber Range technologies, will further enhance the impact of Cyber Ranges on cybersecurity education.

In this ever-evolving cyber landscape, educational Cyber Ranges are vital in ensuring a well-prepared and resilient workforce capable of tackling the future's dynamic and ever-changing cyber threats. By embracing the potential of Cyber Ranges and leveraging their benefits, academic institutions can shape a future where cybersecurity education is immersive, practical, and highly effective in producing skilled professionals who can safeguard our digital world.

Finally, by thoroughly reviewing the capabilities of Cyber Ranges, institutions and instructors can look at maximizing their investments and empowering effective cyber training and learning.

Notes

[1] https://www.comparitech.com/blog/information-security/global-ransomware-attacks/

[2] https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report#1

[3] https://assets.sophos.com/X24WTUEQ/at/k4qjqs73jk9256hffhqsmf/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469

[4] https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf

[5] https://purplesec.us/resources/cyber-security-statistics/

[6] https://techbeacon.com/enterprise-it/counter-security-threats-machine-learning-real-time-data-analytics

[7] https://www.forbes.com/sites/forbestechcouncil/2023/01/27/how-providing-staff-awareness-training-improves-a-companys-security-posture/?sh=31d38e0a5a9a

[8] https://www.theglobeandmail.com/business/adv/article-severe-cybersecurity-talent-gap-creates-vulnerabilities/

[9] https://www.ictc-ctic.ca/news-events/one-in-six-canadian-cybersecurity-roles-go-unfilled-new-report-explores-talent-shortage-and-solutions

[10] https://www.digitalthinktankictc.com/reports/cybersecurity-talent-development

[11] (ISC)² 2022 Cybersecurity Workforce Study https://www.isc2.org/

[12] https://www.usenix.org/system/files/conference/ase16/ase16-paper-yue.pdf

[13] https://www.ibm.com/blogs/ibm-training/new-cybersecurity-threat-not-enough-talent-to-fill-open-security-jobs/?ref=hackernoon.com

[14] https://www.zdnet.com/article/cybersecurity-leaders-want-to-quit-heres-what-is-pushing-them-to-leave/

[15] https://www.growthengineering.co.uk/kolb-experiential-learning-theory

[16] https://www.simplypsychology.org/learning-kolb.html

[17] https://certify.cybervista.net/alternative-pathways-to-a-career-in-cybersecurity/)

[18] https://skopik.at/ait/2022_icissp.pdf

[19] https://cordis.europa.eu/project/id/786668

[20] https://www.nist.gov/system/files/documents/2020/06/25/The%20Cyber%20Range%20-%20A%20Guide%20%28NIST-NICE%29%20%28Draft%29%20-%20062420_1315.pdf

[21] https://cybersecurityguide.org/resources/cyber-ranges/

[22] https://cyber.org/range#:~:text=Students%20are%20able%20to%20get,how%20to%20defend%20against%20them.&text=The%20labs%20in%20CYBER.,for%20the%20CompTIA%20Security%2B%20Exam

[23] https://www.cloudrangecyber.com

Contact Our Team

Email

sales@enfocom.com

Phone

1-888-ENFOCOM

1-888-363-6266

Direct: 403-291-5500

ENFOCOM CYBERSECURITY

About the Author

Edward Rochester, B.Sc., M.Sc., Ph.D. Candidate, has been working as a Security Analyst with ENFOCOM since 2020 and is an active researcher in the field of cybersecurity and data privacy.
Edward will continue his Ph.D. with the University of Calgary focusing on the field of cybersecurity and data privacy while providing valuable insight and innovation to the future of the organizations which he supports.

About Us

ENFOCOM CYBERSECURITY is on a mission to help Canadian organizations protect their data from being stolen or taken for ransom.

With our partners Field Effect, Raytheon Canada and the University of Calgary we are confident that we can lead the way in cybersecurity growth and education with cutting-edge technology of the Cyber Range.

The Cyber Range facilitates training which can be deployed in minutes in the cloud or at our facility. By working with us our customers are always working with the latest technology, products and services that improve their cybersecurity posture better today, than yesterday.

Learn More About The Cyber Range at

ENFOCOM.COM