Create a Cybersecurity Center of Excellence and Culture at the Province of New Brunswick

Published: 18 October 2019 **ID:** G00383594

Analyst(s): Brent Predovich, Earl Perkins

The CyberNB initiative is a pioneering collaboration involving government, academic and commercial participants. This overview of the program's strengths and weaknesses can give SRM leaders a competitive advantage in attracting the best talent, improving awareness and fostering collaboration.

Impacts

- Conflicting communication and engagement between centralized and distributed leadership has led to siloed and uncoordinated actions.
- Lack of project awareness across external and initial stakeholders has led to missed opportunities with attracting new contributions, monetary and otherwise.
- Challenges in capitalizing on skills development have hampered SRM leaders' capacity to remain innovative and bring new ideas into their ecosystem.

Recommendations

Security and risk management (SRM) leaders overseeing cybersecurity development programs must:

- Equip departments with optimal communication by promoting cross-department collaboration, decompartmentalizing meetings and cross-functional stakeholders.
- Inform and prioritize program goals by leveraging real-time security events and intelligence.
- Invest in multitiered and diverse education by growing mentorship, publications and cyber ranges to prepare for future challenges.

Analysis

The New Brunswick CyberNB project is an ongoing attempt at creating a utopian ecosystem for security learning and awareness. The project will have invested CDN$3.8 million by 2020 in an integrated Cybersecurity Innovation Centre supporting a critical infrastructure security operations center (CI-SOC) and IoT innovation and testing.

According to the CyberNB website, "the Province of New Brunswick launched CyberNB in May 2016." It goes on to say that "as part of the Province's economic development agency, Opportunities NB, CyberNB is purpose-built to focus on both economic and societal issues."[1]

Ecosystem partners include Bell, IBM, Siemens and many other private companies. Canadian institutions such as the University of New Brunswick and several other academic schools, law enforcement, and intelligence agencies such as the Canadian Centre for Cybersecurity and Public Safety Canada are participating.

SRM leaders should apply the lessons from the CyberNB project when planning collaboration with public organizations or engaging industry participants.

The stated aims of the project include:

- Collaboration
- Transparency in communication
- High stakeholder engagement
- Strong project governance with strong executive sponsorship
- Establishment of a "sense of purpose" with a focus on the greater good
- Iterative development and delivery
- Adoption of an outsourcing approach
- Exploring and developing a regional threat response capability

The impacts of the program indicate the benefits of collaboration, most notably increased funding and the real likelihood of inconsistent communication across participants — both areas of success and failure for SRM leaders.

Figure 1. Impacts and Recommendations for Province Cybersecurity Awareness and Training Programs

Impacts and Recommendations for Province Cybersecurity Awareness and Training Programs

Impacts	Top Recommendations
Conflicting communication and engagement between centralized and distributed leadership has led to siloed and uncoordinated actions.	• Attract further student and stakeholder participation in other areas by using comprehensive program marketing. • Achieve optimal communication by promoting cross-department collaboration, decompartmentalizing meetings and cross-functional stakeholders.
Lack of project awareness across external and initial stakeholders has led to missed opportunities with attracting new contributions, monetary and otherwise.	• Leverage real-time security events and intelligence to inform and prioritize program goals. • Develop a first responder identity for real-time events to maximize contribution to the global cybersecurity agenda and optimize CyberNB's status.
Challenges in capitalizing on skills development have hampered capacity to remain innovative and bring new ideas into their ecosystem.	• Invest in multitiered, diverse education by growing mentorship, publications and cyber ranges to prepare for future challenges. • Minimize theoretical education and maximize practical education, and implement an education methodology with active scenarios.

Source: Gartner
ID: 383594

Impacts and Recommendations

Conflicting Communication and Engagement Between Centralized and Distributed Leadership Has Led to Siloed and Uncoordinated Actions

One of the CyberNB program's key strengths has been the coalition's ability to remain free of ego or unilateral agendas. Participants pride themselves on their support of partner growth, which reinforces the program's success. Change is a mandate of the mission, and with the right culture in place, the program's ability to grow cybersecurity within the partners and the ecosystem has improved.

The CyberNB program now hosts international summits, and the project has contributed to an overall enhancement of interaction across numerous sectors of the Canadian economy. Along with

a professional development framework, CyberNB has contributed to industrial cybersecurity frameworks such as the Cybersecurity Forum and has increased relationships across three sectors of government. Formal partnerships are in place with the communications establishment, public safety agencies, the Indigenous Skills and Employment Training (ISET) program and the federal ministry. In one leader's view, the biggest achievement is the level of commercialization and operationalization of the CI-SOC initiative.

Other leaders[2] feel that the project must stay true to its roots and build on a collaborative culture. Existing as CyberNB does in a not-for-profit world, there is a compelling need for the program to generate its own revenue and funding. The project needs to stay true to those objectives in order to drive commercialization and collaboration.

The area of improvement most needed culturally is to clarify what CyberNB stands for. Leaders must ensure the organization lives by its mandate and purpose as a coordinating body in government, academia and industry. Leaders must ensure strategic vision; for example, they should access more funding opportunities and increase levels of Pan-Canadian involvement. Recent decisions by the Government of New Brunswick will create a not-for-profit entity to increase access to funding opportunities and ensure Pan-Canadian participation.

Other struggles to date are associated with structural limitations. CyberNB must increase the level of marketing and stakeholder engagement. Participants should spend more time making other industries and government agencies aware of CyberNB. Trumpeting successes, promoting CyberNB's story, increasing the level of dialogue and growing the level of participation with other jurisdictions are all key areas for improvement.

Most participants understand their respective role, but have a limited understanding of what's happening across the entire project. A lack of repeatable processes may limit the ability to replicate successes elsewhere.

Leaders agree that communication could be more regular, connected and cohesive. In terms of talent development, for example, breaking down silos with effective communication is required. These silos are within the sectors of the organization and within industry, academic and government partners.

Recommendations:

- Attract further student and stakeholder participation in other areas by implementing comprehensive program marketing.
- Achieve optimal communication by promoting cross-department collaboration, decompartmentalizing meetings and cross-functional stakeholders.

Lack of Project Awareness Across External and Initial Stakeholders Has Led to Missed Opportunities With Attracting New Contributions, Monetary and Otherwise

The project promises a way to bring young people into technology jobs, though it faces challenges, and an overview of the initiative's strengths and areas for improvement reflect the opportunities such a project can offer a technology community.

According to the project's description, SRM leaders of the CyberNB program said it is designed to create an environment for enabling partners to protect their own clients while collaborating on broader critical infrastructure protection.

> "This innovative project will enable the collaboration required to share intelligence and best practices and provide a central resource for gathering information on cyber threats to critical infrastructure and providing two-way sharing of information between the private and public sector."[3]

While the program has established the necessity for two-way sharing of information among private and public sectors, the overall execution of the task has been a challenge. Note that this challenge is faced because of the difficulty of being able to quantify the execution of the communication.

Some of the project's quantifiable functions include:

- Reviewing the NIST framework for improving critical infrastructure protection and tuning it for Canada
- Developing new intellectual property in the form of working practices, tools and techniques that will form the foundation of a maturity model for SOCs
- Setting the foundations for cybersecurity critical infrastructure protection innovation within Canada
- Constructing a resilient infrastructure for the SOC

Several strengths have become apparent since the project's early days. The project's awareness at national and international levels has gained the CyberNB initiative recognition beyond the eastern Canada region. Leaders observe a higher degree of awareness and interest in Canadian technology practices inspired by CyberNB, including the efforts of the Canadian Nuclear Laboratories team, which fosters technology investment throughout the country.

Bell's commitment has led to the initiative getting additional capabilities that it would not have gotten otherwise. Participant response capabilities have improved with the expansion of collaborative responses to protect critical infrastructure. This awareness echoes the fundamental concept of the program.

For example, if an instance hasn't occurred in a particular environment, uninformed participants have access to information from other organizations that will allow them to comprehensively understand and preemptively prepare for these unknowns before something happens.

Critical events that disrupt the cybersecurity landscape can be leveraged to elevate the awareness and influence of the program. Leveraging these disruptions highlights the program's importance in the modern world. Investment will be necessary from the province and its associated public partners as a key to success (see "Three Critical Factors in Building a Comprehensive Security Awareness Program").

Recommendations:

- Leverage real-time security events and intelligence to inform and prioritize program goals.
- Develop a first responder identity for real-time events to maximize your contribution to the global cybersecurity agenda and optimize CyberNB's status within the community.

Challenges in Capitalizing on Skills Development Have Hampered SRM Leaders' Capacity to Remain Innovative

While expanded collaboration is a common hope for many leaders, SRM leaders of the CyberNB program have shown several strengths since the early days of the project. Partnerships that did not exist in the past have been formed with competitors, and alliances have been built with companies. Business contacts have been formed with bodies in government and academia that have sent their talent to CyberNB to contribute on various issues.

One program leader[4] reports that the project has created opportunities for young people who would not have had the chance to rise to any level of participation or flourish in their environment. Some students have been diagnosed with specific learning disabilities (SLD) or autism spectrum disorder (ADS), yet they exhibit clear ability in coding. Leaders say these young people have "come out of their shells" as they contribute in ways that they never thought they could and experience high levels of success. While providing opportunities for these young people, the program has also established a corporate social responsibility identity within the program and the industry.

Program leaders in the CyberNB initiative[2] are also identifying advanced academic and employable talent. The students discovered by the program are often overlooked in hiring efforts. They are average students with an interest in tech, generally not the "high-flying," but as one leader put it, they are suited for the rigors and challenges of cybersecurity careers. Another CyberNB objective is to develop K-12 students as potential cybersecurity professionals. Linking the different curricula to make a cohesive program has been a challenge.

Program leaders have struggled to train more teachers. Teachers and families have found the concept of cybersecurity hard to comprehensively understand. Some of the concepts are dense; thus, teachers must identify how to make it more interesting and fun, how to appeal to more learning styles, and how to teach appropriately. There is also no guarantee of financial gain for participants, which one official speculates is why academia has shied away from full participation.

Bringing academia, corporations and government together is difficult. The expectation is not that government agencies would lead such efforts. Historically, even intelligence agencies had a problem with sharing information. SRM leaders of the CyberNB program must establish the identity of the program as an academic, nonprofit organization with the authority of a government agency.

Competition in this space is intense. SRM leaders of the CyberNB program must overcome this obstacle in order to collaborate. They must decentralize stakeholders with lateral collaboration to the education program, while implementing a "co-opetition" mindset among external parties. This coalition has helped build an important network that can drive the type of learning that comes through hosted workshops.

Innovative ideas have not yet come to the fore. Innovation will come when participants share data, especially around critical infrastructures, processes, incidents and governance. Leaders feel that greater intelligence sharing through the coalition will help.

Recommendations:

- Invest in multitiered and diverse education by growing mentorship, publications and cyber ranges to prepare for future challenges.
- Develop data sharing agreements, trusted collaborative systems and more automated functions.
- Minimize theoretical education and maximize practical education, and implement an education methodology with active scenarios.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Three Critical Factors in Building a Comprehensive Security Awareness Program"

"Critical Elements for Your Security Program's Success"

"Designing a Security Champion Program"

"Hiring the Right Talent to Run Your Security Awareness Program"

Evidence

[1] CyberNB website

[2] Based on feedback we received in a series of interviews with Tyson Johnson, chief operating officer of CyberNB.

[3] "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology.

[4] Adam Binet, Cyber Defense Hub Government of New Brunswick

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp