1G
CYBER

ORGANISATION & METHODOLOGY

1. RATIONALE

1GCYBER submits a proposal that will add value to Latin America and the Caribbean. Our influence for this proposal stems from Mr. Fraser's research on "Cybersecurity skills as a driver for economic growth in developing nations." This research explores the current issues prohibiting skills development, cybersecurity challenges, and the impact of cybercrime on national economic sectors. 1GCYBER specifically seeks to strategically deliver on key challenge areas: a) limited regional cybersecurity skills b) national and regional cybersecurity challenges, c) how cyber-crime impacts each regional state, and d) existing legal structures and gaps for operational management. These four themes will tactically serve as a light house towards which the training will be delivered to prepare highly trained practitioners.

The proposed courses will help to conjure critical thinking about the region's future cybersecurity needs as Latin America and the Caribbean advances economic and national security. As a known national imperative, the ability to combat cyber-crime and strengthen cyber resilience is essential to improving national economic and social development. The existing risk management frameworks echo economic security as a foundational pillar for domestic growth. Cybersecurity addresses the inherent risks to critical infrastructure and services resulting from the use of information and communication technology. The developed nations, specifically the United States, Britain, and Canada, recognize the importance of critical infrastructure systems. They continuously develop strategies that include cybersecurity education as a measure to protect cyber-physical systems.

The lack of a workforce with the requisite cybersecurity skills is a phenomenon that exist within the region and that which 1GCYBER commits to support through superior training. COUNTRY PROGRAMS's focus on cybersecurity skills forms the necessary foundation to correcting the current cybersecurity challenges and impact of cybercrime on the region. The issue varies from country to country. However, each presents a case that fosters critical thinking, influencing decision making and policy. This training proposal stems from a thorough understanding of the elements set forth in the Caribbean Cyber Security and Cybercrime Action Plan. 1GCYBER will ensure that all participants understand cybersecurity through the doctrine of risk management. The proposed curriculum will adequately address the system dynamics of cybersecurity, cybercrime, education, and national security functions.

Professionals in Latin America and the Caribbean will leave with the requisite knowledge, skills, abilities, and core competencies to adopt and implement recommended best practices. 1GCYBER will ensure that training addresses these thematic elements from a global and CARICOM Community perspective. Apart from training and sharing of experiences, the proposed courses will draw attention to the need for knowledge about the instrumental value cybersecurity skills offer CARICOM. Policymakers, stakeholders, educators, and citizens of the region, and other similar developing countries will benefit from this opportunity. 1GCYBER will seek to influence a regional cybersecurity community, through services that encourage participating professionals to continuously collaborate, study, and work on their administrative and technical

cyber capabilities. Apart from the proposed training, participants will be encouraged and given relevant resources to pursue certification, which serves as an attestation to their new abilities.

1GCYBER understands the regional skills and technical resource landscape. We anticipate there will be a mixture of skilled professionals and will make modifications to the proposed curriculum based on the average capability. This risk will be managed early by ensuring all participants across the two lots are given core knowledge, skills, and abilities (KSA). 1GCYBER's training is influenced by the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework and the Chartered Institute of Information Security's knowledge, skills, and roles frameworks.

1GCYBER will also encourage leadership and teamwork as a form of developing those non-technical skills that the literature critique as missing from current frameworks. Participants will be encouraged to complete free industry training from edX (Linux), Splunk (Reporting), and AWS (Cloud). These serve as essential knowledge and inputs to the Advanced Cybersecurity Skills Framework but are not a mandate. The proposed courses will implement these structures. Another vital risk to address is participant computing devices. Participants must have devices capable of installing virtualization technology, and Linux and windows virtual systems. 1GCYBER will address this risk by encouraging teamwork, in Zoom breakout rooms, where all participants collaborate on lab work.

2. STRATEGY

A trainer led video or machine tutoring systems facilitate robust learning for long-term retention, fact transfer, and future references. When compared to live conventional classroom instruction for technical domains this guidance often fall short of well-structured curriculum delivery. Although different instructional strategies can be used to deliver training, a human expert in a live classroom setting ensures quality discourse and learning outcomes. 1GCYBER will deliver instructor led training and employ several delivery methods based on the curriculum and dynamic experiences in the cohorts. This will address the classic example-problem dimension of the assistance dilemma when individuals learn.

1GCYBER will employ three instructional strategies: examples only, examples-problems, and problems only to bringing participants current knowledge, skill, and abilities to a desired or potential level. This approach will strategically implement the prior mentioned risk factor. The three bracketed approach will explore participants cybersecurity KSA and problem-solving abilities, as a measurement of prior experience and skills. 1GCYBER has researched this area will measure capabilities using criteria and formulas.

1GCYBER will use test-based surveys, questionnaires to collect knowledge and skills data across the workforce. The questionnaire tool evaluates standards such as the UK Cyber Security Essentials. This approach characterizes attributes across coded rating scores for responses relative to the training's objectives. The feedback data will serve as inputs to the computation stage of the evaluation model. Table 1. presents the capability ratings, range, and priority ratings based on security responses in questionnaires.

Table 1

Capability – priority range table

Capability rating	Capability range	Priority rating *(Security response)*
Low *(l)*	$0 \leq l \leq \frac{1}{3}$	High
Moderate *(m)*	$\frac{1}{3} < m \leq \frac{2}{3}$	Moderate
High *(h)*	$\frac{2}{3} < h \leq 1$	Low

Note. Reprinted from Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. Journal of Systems and Information Technology, 21(1), 2–35. doi:http://franklin.captechu.edu:2123/10.1108/JSIT-02-2018-0028

The National Cyber Security Centre provides risk management consideration for home and work, incident management, network security, malware prevention, managing users, monitoring, removable storage, secure configuration, and user education. The considerations support security decisions and help orient professionals on security objectives. 1GCYBER will apply mathematical procedures to enumerate workforce capability values from the knowledge and skills data. The formulation process assumes p is an employee in P, the workforce. Figure 1. shows how to calculate the cumulative knowledge capacity (CKC) for p in P calculates:

$$Kc_p = CKC_P = \left[\sum_{x=1}^{5} (x.n_x)\right]_p, \ \forall \ p \in P$$

Figure 1. Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. Journal of Systems and Information Technology, 21(1), 2–35. doi:http://franklin.captechu.edu:2123/10.1108/JSIT-02-2018-0028

Figure 2. shows how to calculate the cumulative skills capacity (CSC) for p in P calculates.

$$Sc_p = CSc_P = \left[\sum_{y=1}^{5} (y.n_y)\right]_p, \ \forall \ p \in P$$

Figure 2. Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology, 21*(1), 2–35. doi:http://franklin.captechu.edu:2123/10.1108/JSIT-02-2018-0028

This adopted method supports aggregating the data about the participating workforce security capacity, evaluating the responses, and benchmarking context-driven cyber threats to the

organization. Figure 1. and Figure 2. compute knowledge and skills, which harmonize into the personalized security capability (PSC). The PSC uses a geometric mean technique to determine the employee's knowledge and skill score since it removes the skewness influence of large values by normalizing totals and ensuring either weight does not influence the result. Figure 3. shows the calculation of the geometric mean score from the CKC and CSC.

$$PSC_p = \left(Kc_p \times Sc_p\right)^{1/2}, \ \forall\ p \in P$$

Figure 3. Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. Journal of Systems and Information Technology, 21(1), 2–35. doi:http://franklin.captechu.edu:2123/10.1108/JSIT-02-2018-0028

Organization and Methodology

1GCYBER will use a Bootcamp approach to curriculum delivery. Bootcamp program delivery focus on several vital areas of consideration: academic rigor, cost, prior skills, temporal dimension, and fast learning outcomes. 1GCYBER has been researching and practicing this delivery method and use participant data to answer questions about the learning among cohorts who have limited to advance knowledge in the domain. Do professionals acquire an in-depth understanding of KSAs as core abilities to lead specific job roles? A live in-person training, as offered in Bootcamps, helps empower professionals to learn through discovery and reduces mistakes, addressing the competency gap. The quality and depth of learning are factors that impact how much KSA participants acquire in this immersive learning environment. However, experience will address this at the beginning of each course delivery.

Gathering relevant participant data on KSAs at the beginning of each training (current state), during (quizzes, procedures, discussions as operators), and at the end (projects as target state) will describe the expertise acquired. A Knowledge-Lean and Knowledge-Rich planning approach will support participants and trainers to obtain dynamic solutions, even if participants do not have initial abilities to solve problems with both limited and extensive knowledge. 1GCYBER practices the *Knowledge-Lean* plan that uses *P* as a tuple in *(F, I, O, G),* where *F* describes the students in the Bootcamp environment. The component *I* will be their current or initial state while *O* is the set of learning instructions or operators provided by the curriculum over the period. The *G* is the formula over *F* that describes learning outcomes at the end of the training. The target state *G* will be achieved once the operators *O* are adequately applied from the initial state *I*, addressing *P* – cybersecurity skills training in the Bootcamp learning environment for CARICOM Professionals.

Table 2

1GCYBER's Proposed Approach to Cybersecurity Skills Development

TACTICAL	OPERATIONAL	STRATEGIC
• Introduction to Cybersecurity • Awareness • Community Work and Challenges • Legal and Regulatory Frameworks	• Enterprise Technology • Hands-on labs • Technology used in Heterogeneous Environments • Self-Study	• Knowledge • Skills • Abilities • Competency • Confidence • Vocabulary

This approach will ensure professionals acquire the requisite administrative and technical skills. Bootcamps are one alternative to curriculum delivery. 1GCYBER will analyse the entry and exit criteria and learning process to glean the learning outcomes of participants. Figure 4. provides a strategic training outline aligned with the cybersecurity knowledge for education, job roles, and responsibilities. Participants in Lot One will complete all work in the below model, while those in Lot Two will focus primarily on Legal and Regulatory Frameworks.

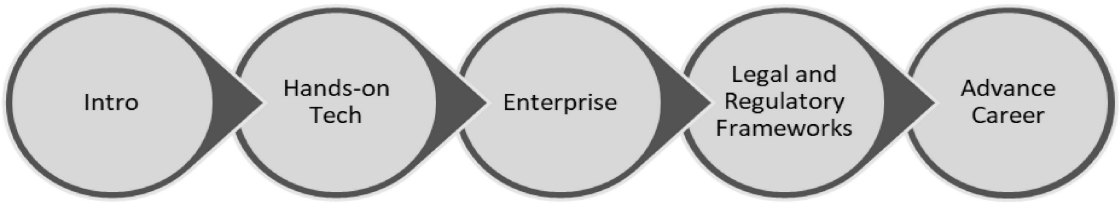

Figure 4. Cybersecurity Bootcamp Training & Curriculum Delivery. © Copyright 2021 1GCYBER. Registered in England: number 13288834.

The below Advanced Cybersecurity Skills Framework will be the total of expected capabilities participants learn over the training period. 1GCYBER's Director, Fraser, developed this chart while training hundreds of professionals across mixed learning environments. The methodology has produced scores of industry certified professionals who now contribute to cyber organizations in the United States. Figure 5. serves as a road map to the previously discussed light house that will deliver core skills across the cyber security kill chain and Cybersecurity Framework. These skills will be individually developed as participants collaborate to model a

virtual enterprise environment – through information and technology asset acquisition, installation, configuration, assessment, and monitoring.

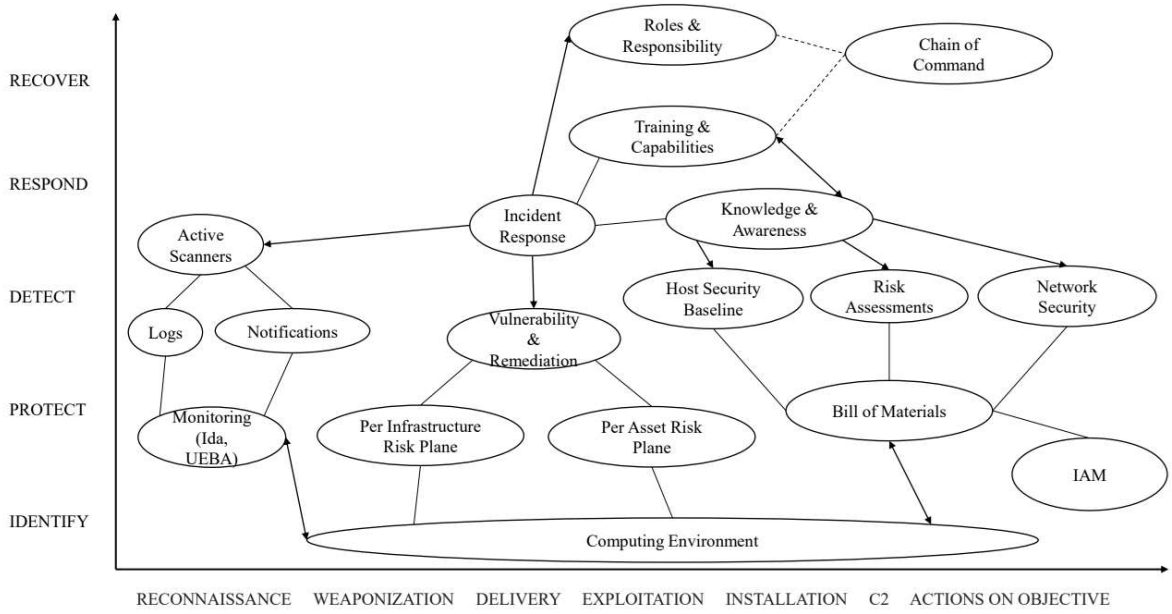

Figure 5. Advanced Cybersecurity Skills Framework. © Copyright 2021 Cyber Benab Limited (1GCYBER). Registered in England: number 13288834.

Core Curriculum Topics

The shifting landscape of threats and vulnerabilities require organizations and professionals to continuously invest in cybersecurity skills. The input and output of job duties are individual competencies. A competent workforce is the cornerstone of a secure cyberinfrastructure. This protects an organization's assets and economic interest while ensuring cost avoidance. Table 3. identifies several examples of core skills development areas.

Table 3

1GCYBER's Proposed Core Skills Focus

Course	Deliverables	Outputs
Network Administration/Security	● Acquire, install, and configure networking devices – routers and switches using subnetting. ● Knowledge of TCP/IP and OSI models to analyse network activity with tools like Wireshark.	Participants will develop core KSAs to perform network administration and security tasks.