FUNDAMENTALS OF CYBER SECURITY (FOCS)

DATES	LOCATION	COST
April 29-30, 2020 May 27-28, 2020 June 17-18, 2020 September 23-24, 2020 October 28-29, 2020 November 18-19, 2020	**Ottawa, Ontario** Metcalfe Hotel (123 Metcalfe Street) or Lord Elgin Hotel (100 Elgin Street)	2 Days $2,200 + HST

COURSE SUMMARY *(This course is one of the essential courses required for **certification and designation as a Security and Resilience Professional/Manager** under the Infrastructure Resilience Research Group, IRRG, Office of the Dean, Faculty of Engineering and Design, Carleton University.)*

This course has been specifically designed for employees and managers gain and advance understanding and knowledge to communicate and participate in discussions with IT and ICS experts to address the growing cyber security threats to organizations and digitalized infrastructure systems.

The course is divided into the following four (4) modules:

Module 1: Security in the Digital Age
Builds on the understanding gained from Module 1 and discusses the cyber security threat landscape and organizational vulnerabilities, including sabotage; inside threat, etc.

Module 2: Cyber Attacker Tradecraft
Discusses recent cyber incidents and their impacts on organizations, how attackers exploit small system vulnerabilities to escalate their access and steal classified/confidential information.

Module 3: Cyber Security Controls
Will cover open sources collection of intelligence techniques/cycles, social engineering types of information available to carry out personnel assessment, understanding criminal mindset, modern warfare, cyber security culture, and best practices.

Module 4: Cyber Security Terminologies and Concepts
To be able to participate in cyber security incidents discussions, one needs a clear understanding of the various terms that are used. This section will explain in non-technical concepts, such as: network architecture, virus, ransomware, SUTNET, cybercrime, IOT, VPN, cloud, exploits, firewall, data breaches, malware, Trojan house, worm, bot/bot net, DDOS, phishing/spear phishing, encryption, BYOD, clickjacking, pen-testing, domain, software, etc.

At the end of the course, you will be able to:

- Use OSINT to supplement reliability screening reviews and investigations;
- Recognize the exposure from information publicly available to attackers;
- Explain at a high level the steps behind a cyber attack;
- Express and evaluate cyber risks as business risks;
- Communicate requirements and comprehend feedback from IT personnel with regards to cybersecurity; and
- Explain the rationale behind basic and specific IT security controls.

Upon the successful completion of this training, the course participants will be issued an IRRG certificate, indicating that they have gained the required fundamental knowledge to cybersecurity.

Who should attend:

This course is designed for security managers and practitioners advance their understanding of IT/ICS security in order to engage in effective communication and resolve issues with respect to information and cybersecurity.

Security professionals, from Government and the Industry, who have to interact with their organization's IT, ICS control room supervisors, officials, and require basic underlining of the threats and techniques to be able to participate in discussions.

Managers responsible for addressing their organization's cybersecurity issues.

Generalists interested in gaining awareness of the growing cybersecurity threats and concepts.

COURSE INSTRUCTOR:

- Antoine Lemay, Ph.D., CISSP, GSEC, GCIH
  Chief Training Officer, Cyber Defence Corporation

March 2020