Certificate, Diploma and Nanodegree Online Enterprise Cybersecurity Education covering Policy, Management, Technology, and Digital Forensics

Developed and Prepared by
First Atlantic Cybersecurity Institute
7429 Lighthouse Pt, Pittsburgh, USA
www.facyber.com

Email: facyber@fasmicro.com

Introduction

With the advent of dangerous malicious codes like Flame and Stuxnet, it has become evident that cybersecurity poses existential threats to institutions if not properly managed. As the risks of traditional wars abate, Internet has since evolved as the 21st century battleground where malware, not rockets, can be used to launch attacks on infrastructures like power, telecoms, capital market and financial institutions. Also, through espionage and hacking, organized crimes by nations, corporate institutions and individuals can steal vital intellectual properties (IPs) that drive innovations in any economy. When a country or an organization loses its competitive advantage, its market-winning capability will be weakened. Besides the malwares and worms, there is also the human element which poses risks to intellectual properties and business trade secrets owing to the ease to move digital wares. Our training programs are designed to equip learners with 21st century cybersecurity and digital forensics skills that will help them advance their careers and master major ways to Prepare, Detect, Defend, Defeat, and Harden their organizations' critical digital and information assets.

Cybersecurity is not a game of choice – it is the new normal. Unlike in the past, modern hackers are coordinated, well-funded and operate like corporations. The Central Bank of Nigeria has noted that Nigerian financial institutions are losing millions of dollars to cybersecurity related frauds and threats. The 21st century will be a century of cyber warfare and will require strategic readiness for organizations. These institutions have to plan beyond dependence on state institutions for cybersecurity protections. Across Nigeria, the level of that preparation to secure and protect assets like power systems, telecoms, financial infrastructures, water systems, and more are still evolving.

Furthermore, the world has nuclear non- proliferation treaty, but none exists for cyberwar despite the potential economic dangers the latter poses to world commerce. Accordingly, many nations have started to deploy strategic commands to protect, defend and necessarily retaliate when their systems are attacked through cyber-means. The United States Pentagon has the Cyber Command inside the National Security Agency, the British has a similar unit inside the GCHQ. China, Iran, Russia, Israel, and many other nations have developed cyber-army to protect their economies. Our programs are designed to also help develop cybersecurity manpower for state institutions and governments. These institutions could be law enforcements, military, and industry regulators.

Our Firm, First Atlantic Cybersecurity Institute, works with organizations to deepen their internal cybersecurity and digital forensics capabilities by training their workforce. We also provide cybersecurity research and consultancy. Our programs cut across Cybersecurity Policy, Cybersecurity Management, Cybersecurity Technology and Cybersecurity Intelligence / Digital Forensics structured along Certificate, Diploma and Nanodegree programs. We have operated via Milioncs Analytics, an IBM PartnerWorld, and worked for government agencies like National Identity Management Commission (NIMC) and Nigerian Electricity Regulatory Commission (NERC) in addition to banks and insurance companies. Recently, we unveiled a portal (www.facyber.com) dedicated to cybersecurity/digital forensics education and training.

Program Objectives

ICT is facilitating the process of socio-economic development of nations. It has offered new ways of exchanging information, and transacting businesses, efficiently and cheaply. It has also changed the dynamic natures of financial, entertainment and communication industries and provided better means of using the human and institutional capabilities of countries in both the public and private sectors. Increasingly, ICT is rapidly moving nations towards knowledge-based economic structures and information societies, comprising networks of individuals, firms and nations that are linked electronically and in interdependent relationships. As economic systems go digital, the risks posed by unsecured weakest links in financial systems at host, intermediary and client levels will become prominent.

Through digital combats in Estonia and Ukraine, it has been established that cyber-threats are not games of choice. As internet penetration continues to advance globally, so are the perils that come with the increased degree of digital connectivity. However, most organizations lack both proper security plans and trained in-house staff to counter or quickly recover from cyber attacks.

The goals of FACYBER programs are to:

- Develop business and government leaders with competence to create and manage effective cybersecurity practices
- Understand and solve the evolving cybersecurity risks, equipping learners with cutting-edge skills in a fledgling industry even as nations/firms move into electronic societies with associated digital risks
- Prepare learners to master ways to Prepare, Detect, Defend, Defeat, and Harden their critical information infrastructure
- Prepare learners to have ability to develop national and enterprise cybersecurity policy, strategy and governance frameworks
- Make excellent cybersecurity managers and policymakers across core areas of cybersecurity and digital forensics

Our course presents basic and advanced concepts in cybersecurity, forensics and digital security management. Topics cover cybersecurity technology, cyber policy, digital forensics, information assurance, cyber investigation and malware analysis. Presented with mix of technology, management and policy, the following areas are covered: business continuity management, protocols, OS security, vulnerabilities, architecture, cyber services, algorithms, hardware, software, languages, cyber mechanisms, policy, physical security, malware analysis tools, cyber terrorism, cyber espionage, national security and live labs.

Participants to our programs have included IT leaders, Bankers, Insurers, Lawyers, Engineers, Technologists, CEOs, Military, Law Enforcement, Students, Managers, Policymakers, Compliance Officers, Regulators, and more.

Program Structure/ Cost

Our Cybersecurity education is structured around four key pillars of policy, management, technology and digital forensics. This implies that we cover all the core needs of any organization or state institutions. While some staff like corporate lawyers may require training on policy, some staff like IT managers may need technical skills. Others like business leaders will

find the management module useful. We deliver all these programs through our web portal – www.facyber.com. The program structure is presented below: certificate programs take 12 weeks; diploma programs which require certificate programs as perquisites take 24 weeks (inclusive of the certificate programs) and the nanodegree programs require a live (physical) one week training in Lagos (for Nigerian learners) with the diploma programs as prerequisites.

Core Modules Week 1 – Structure of Information Systems Week 2 - Information Systems & Networks Vulnerabilities Week 3 - Foundations of Cybersecurity Week 4 – SMAC & BYOD Security Week 5 – Preventing Cyber Intrusions Week 6 – Evaluating Emerging Cybersecurity Technologies		
CYBERSECURITY CERTIFICATE PROGRAMS		
Programs	Descriptions	Duration
Certificate in Cybersecurity Policy (CCYP)	Week 1 – 6: See Core Modules above Week 7 - Ethics in Information Technology Week 8 - Security Policy Analysis Week 9 - Security Policy Implementation Week 10 –Global Cybersecurity Policy & Law Week 11 - Enterprise Cybersecurity Policy Week 12 –Exam	12 weeks
Certificate in Cybersecurity Technology (CCYT)	Week 1 – 6: See Core Modules above Week 7 - Ethical Hacking Week 8 - Malware Analysis Week 9 - Penetration Testing & Tools Week 10 - Intrusion Detection and Prevention Week 11 – Networks and OS Security Week 12 –Exam	12 weeks
Certificate in Cybersecurity Management (CCYM)	Week 1 – 6: See Core Modules above Week 7 - Physical & Human Security Management Week 8 –Cybersecurity Essentials for Leaders Week 9 - Cyber Incident Analysis and Response Week 10 - Building Secure Enterprises & Organizations Week 11 – Cybersecurity Project Management Week 12 – Exam	12 weeks
Certificate in Cybersecurity Intelligence & Digital Forensics (CCDF)	Week 1 – 6: See Core Modules above Week 7 - Digital Forensics & Evidence Week 8 – SMAC & BYOD Forensics* Week 9 – Guarding Against Cyber Intrusions Week 10 –Information Systems Security & Assurance Week 11 – Cyber Intelligence & Counter-Intelligence Week 12 - Exam	12 weeks
	CYBERSECURITY DIPLOMA PROGRAMS	
Diploma in Cybersecurity Policy (DCYP) Diploma in Cybersecurity Technology (DCYT) Diploma in Cybersecurity Management (DCYM) Diploma in Cybersecurity	The equivalent certificate program is a prerequisite. It requires a project or capstone where the participant will take up a project and complete. Previous learners have used the capstone to work on enterprise cybersecurity governance framework, enterprise cybersecurity policy, review of enterprise cybersecurity strategy, development of company cybersecurity policy/strategy, implementation of anomalous occurrence detection systems, etc.	24 weeks (inclusive of the 12 weeks of certificate program)

Intelligence & Digital Forensics (DCDF)	The goal is for the learners to work on something which will have real impact and beneficial to sponsoring institutions. FACyber instructors work with learners throughout the process	
	CYBERSECURITY NANODEGREE PROGRAMS	
Nanodegree in Cybersecurity Policy (NCYP) Nanodegree in Cybersecurity Technology (NCYT) Nanodegree in Cybersecurity Management (NCYM) Nanodegree in Cybersecurity Intelligence & Digital Forensics (NCDF)	The equivalent diploma program is a prerequisite. It requires attending one week live (physical) training in Lagos. This live program is available twice per year and is run by FACyber team.	7 days (requires successful completion of equivalent diploma program)

Program Descriptions

Certificate in Cybersecurity Policy (CCYP): Certificate in Cybersecurity Policy deals with the policy analysis and implementation aspects of cybersecurity. It presents theory and topical issues, at government and enterprise levels, with both technical and managerial components in the fields of information systems security. The program helps learners develop skills on the policy, ethical, and legal issues associated with cybersecurity and information security.

Diploma in Cybersecurity Policy (DCYP) Capstone: This is a practical-oriented program where learners are tasked with developing solutions for a theoretical or real case cybersecurity policy issue with the guidance of a mentor. A project report is required at the end of the program.

Certificate in Cybersecurity Technology (CCYT): The Certificate in Cybersecurity Technology is designed to provide learners with skills to analyze multi-faceted complex cybersecurity issues, develop capabilities to make strategic decisions to protect organizations from threats and become competent cybersecurity professionals.

Diploma in Cybersecurity Technology (DCYT) Capstone: This is a practical-oriented program where learners are tasked with developing capabilities in the core technical aspect of cybersecurity. Learners will have access to some tools and equipment to work throughout this program. A project report is required at the end of the program.

Certificate in Cybersecurity Management (CCYM): The Certificate in Cybersecurity Management equips and prepares learners with modern skills to become effective managers across the broad nexus of cybersecurity and intrusion preventions in organizations. The central core is developing capacity to prevent anticipated cyber intrusions, using experiences to mitigate future threats, and formulating and implementing enterprise-level cybersecurity roadmaps. The program also explores the roles of regulation, policy developments, legal instruments and civil liberties.

Diploma in Cybersecurity Management (DCYM) Capstone: This is a practical-oriented program where learners are tasked with developing cybersecurity project management capabilities with the guidance of a mentor. Here, learners develop cybersecurity implementation frameworks. A project report is required at the end of the program.

Certificate in Cybersecurity Intelligence & Digital Forensics (CCDF): The Certificate in Cybersecurity Intelligence & Digital Forensics is structured to provide modern skills to those interested in digital forensics, digital intelligence and uncovering digital evidence. The program equips learners with broad analytical frameworks and prepares them to become competent cyber investigators.

Diploma in Cybersecurity Intelligence & Digital Forensics (DCDF) Capstone: This is a practical-oriented program where learners are tasked with developing capabilities in digital forensics, digital evidence and digital intelligence. Learners will have access to some tools and equipment to work throughout this program. A project report is required at the end of the program.

Cybersecurity Equipment and Tools

Each participant will need Internet access for the programs. Our firm will provide all the virtual tools and staff facilitators required for the training in our platform. Some of the virtual tools are:

- Virtual Lab Environment: A virtual lab environment employs the concept of virtualization and allows one to use a single physical computer for hosting multiple virtual systems, each running a potentially different operating system
- Computer Forensics Tools: Computer forensic tools are used for digital image acquisition, analysis, reporting, recovery and investigation of material found in digital devices
- Malware Analysis Tools: Malware analysis tools are used to disassemble, debug and analyze compiled malicious executables. This is a key tool in reverse engineering and facilitates malware analysis. While analysis relies primarily on the expertise of skilled and trained personnel, these tools enable the process to be accomplished much easier.
- Live Memory Forensics Tools: Memory forensics tools are used to acquire and/or analyze a computer's volatile memory (RAM)
- Network Forensics Tools: Network forensic tools provide real-time network forensics and automated threat analysis solutions
- Expert Witness Testimony: To provide expert witness testimony, one must be able to provide a visual presentation of associations and linkages that may exist for any person, location or thing under investigation
- Up-to-Date Threat intelligence: Serve as the operational focal point for up-to-date threat information sharing through a Virtual Collaborative Information Sharing Environment for eligible subscribers.

Our Company

First Atlantic Cybersecurity Institute (FACyber) is a wholly-owned subsidiary of FASMICRO Group, a USA-based company. FACyber delivers cybersecurity training/education, research and

consultancy services. Fasmicro Group also owns a wholly-owned Milonics Analytics, an IBM PartnerWorld in cybersecurity and big data analytics that operates in U.S. and across Africa. In 2013, Fasmicro Group was honored by the World Economic Forum (WEF) when the Founder, Prof Ndubuisi Ekekwe, was recognized as a Young Global Leader and the African Leadership Network bestowed upon him a "New Generation Leader for Africa". Fasmicro Group owns a local business in Nigeria – First Atlantic Semiconductors & Microelectronics which develops sensors for farmers.

Payment and Bank information (Nigeria)
UBA – 1019195493
GTBank - 0114016493
Company Name: First Atlantic Semiconductors & Microelectronics
124A Okigwe Rd, Owerri, Imo State, Nigeria /08107116861, 08036613606
Our portal supports Paypal, Visa, MasterCard, Discover and all major global payment systems.

Nigerian Students: Upon Payment, please contact facyber@fasmicro.com so that you can be enrolled to the program with your preferred email address. You can enroll directly at www.facyber.com but you will be required to pay the full program fees. To get the discount, pay offline and send your email address to facyber@fasmicro.com. Below is a sample certificate.