CYBERSECURITY & DIGITAL FORENSICS COURSE MODULES

Mitigate cyber threats Singapore faces in our quest to be a smart nation. IT security professionals are in high demand to help Singapore succeed in this quest. With rapid growth in the area of Financial Technology, information security will be even more critical to protect our financial institutions, Join the fight against cybercrime with our Diploma in Cybersecurity & Digital Forensics (CSF).

In your first year, you will build a strong foundation in basic IT and security through modules such as Programming, Cyber Security Fundamentals, Front-end Development, Databases, Cryptography and Operating Systems Fundamentals.

In your second year, you will develop skills in the areas of network security, software security and digital forensics. You will learn to set up secure web servers, develop secure software applications and investigate cybercrimes. You will also learn how to secure codes and processes that go into developing applications, so that they are protected from external threats right from the start. This is called the Security Development Lifecycle, and is a highly valued skill in the industry.

In your final year, you will put your skills into practice by performing penetration tests on software, systems and networks, conducting in-depth forensic investigations on digital devices and networks, and analyzing malicious software or malware. You will get to do all these as well as work on information security projects in cutting-edge CSF labs.

What's more, you will attend masterclasses by information security professionals, and hone your skills in the real world with internships at the Ministry of Home Affairs and leading IT security organisations, such as Palo Alto Networks, SecureAge, Microsoft, NCS, CrimsonLogic, KPMG, Ernst & Young, CSIT and Ensign Infosecurity. You can also attain the highly sought-after CompTIA Security+ professional certification.

LEVEL 3.1

Ethical Hacking

This module aims to develop Penetration Testers for the information security industry. They will be taught to follow a process model to locate and establish targets, find vulnerabilities, and exploit the flaws to determine potential impact and business risk with the goal of helping the owner improve security practices.

Students will learn the techniques hackers use to hack a system, and the steps to secure it. Students will have hands- on practice on actual pen-testing that involves reconnaissance to map out IT infrastructure, scanning vulnerable systems, and developing attack vectors to exploit loopholes in a system. Students will also be taught the necessary countermeasures to mitigate risks of exploitation through system hardening, intrusion detection and prevention.

Network Security

This module provides an in-depth knowledge on network security in a defensive view. It covers various types of firewall technologies, Virtual Private Networks (VPNs), and Intrusion Detection/Prevention Systems (IDS/IPS). Students will have a chance to configure and deploy state-of-the-art networking devices in a typical computer network.

Students will be taught skills to identify the internal and external threats against a network and to propose appropriate security policies that will protect an organisation's information. Students will also learn how to implement successful security policies and firewall strategies in this module.

Fundamentals for IT Professionals III

This module provides a stepping stone to the students in their IT career. Students are given an insight into the infocomm industries and are kept updated with the latest skill sets required in their IT career path. They also have the opportunity to be exposed to various institutes of higher learning to further acquire their skill sets.

ELECTIVE MODULES

Capstone Project

In this module, students are required to complete a substantial project that is the culmination of their education in the School of InfoComm Technology. The project can be a real-world problem proposed by a client, or it can be proposed by students in pursuit of their personal interests.

Governance & Data Protection

This module examines the relevant frameworks to ensure that information assets are protected within an organisation. It includes the processes and policies for administering and managing a company's IT systems that follow the compliance framework. Concepts on risk management process, risk analysis and mitigation will also be introduced. Students will learn to evaluate risks against the company's critical assets and deploy safeguards to mitigate them. Control frameworks such as PCI (Payment Card Industry), ISO 17799/27002, and COBIT will be covered.

Mobile Device Security & Forensics

This module covers techniques and tools in the context of a forensic methodology to extract and utilise digital evidence on mobile devices. Students will learn how to use current forensic tools to preserve, acquire & examine data stored in a mobile device. The module covers basic SIM Card examination and cell phone forensics on multiple platforms such as iPhone, Android & Windows Mobile. The module takes a practice- oriented approach to performing forensics investigation on mobile phones. This module carries a co-requisite: Digital Forensics.

Network Forensics

Network equipment, such as web proxies, firewalls, IDS, routers, and even switches, contain evidence that can make or break a case. This module provides students with the knowledge and skills to recover evidence from network-based devices. It will begin with an introduction of different network devices and the type of data that are useful from a forensic point of view. It then moves on to the most common and fundamental network protocols that the forensic investigators will likely face during an investigation. These include the Dynamic Host Configuration Protocol (DHCP), Network Time Protocol (NTP) and Microsoft Remote Procedure Call (RPC) protocol. The students will learn a variety of techniques and tools to perform sniffing and log analysis on the network. Commercial and Open Source tools will be used to perform deep packet analysis while SIEM tools such as Splunk will be used to perform log analysis on network devices.

LEVEL 3.2

Internship or Project

This module provides students with the opportunity to apply the knowledge and skills gained to develop an IT solution to solve a practical problem. Students may undertake an in-house industry-driven project or a real- life IT project in a local or overseas organisation. These projects may include problem definition, requirements analysis, design, development and testing, delivery and presentation of the solution. Through the project, students will learn to appreciate the finer points of project planning and control issues relating to IT project development.

COURSE CURRICULUM

Module Name	Credit Units
YEAR 3	
Level 3.1 (22 hours per week)	
Ethical Hacking	4
Network Security	4
Capstone Project or 2 Elective Modules #	8
Fundamentals for IT Professionals III	2
Interdisciplinary Studies (IS) elective ^	2

ELECTIVE MODULES

Governance & Data Protection
Mobile Device Security & Forensics
Network Forensics

Level 3.2	
Internship or Project	22

Notes:

^ For more details on Interdisciplinary Studies (IS) electives, please log on to www.np.edu.sg/is/

IS Module

The School of Interdisciplinary Studies (IS) delivers a broad-based curriculum, which nurtures a new generation of professionals with multidisciplinary skills and an innovative and entrepreneurial spirit to meet the challenges of a knowledge economy. IS offers both prescribed modules and electives to challenge boundaries. Prescribed modules develop students' competencies in core areas such as Communication, Innovation and Enterprise, Culture and Communication, and Personal Mastery and Development, while elective modules provide insights into Arts and Humanities, Business, Design, and Science and Technology.

The elective modules offered may change from year to year, depending on relevance and demand. They may also include modules available in other diplomas offered by the School.