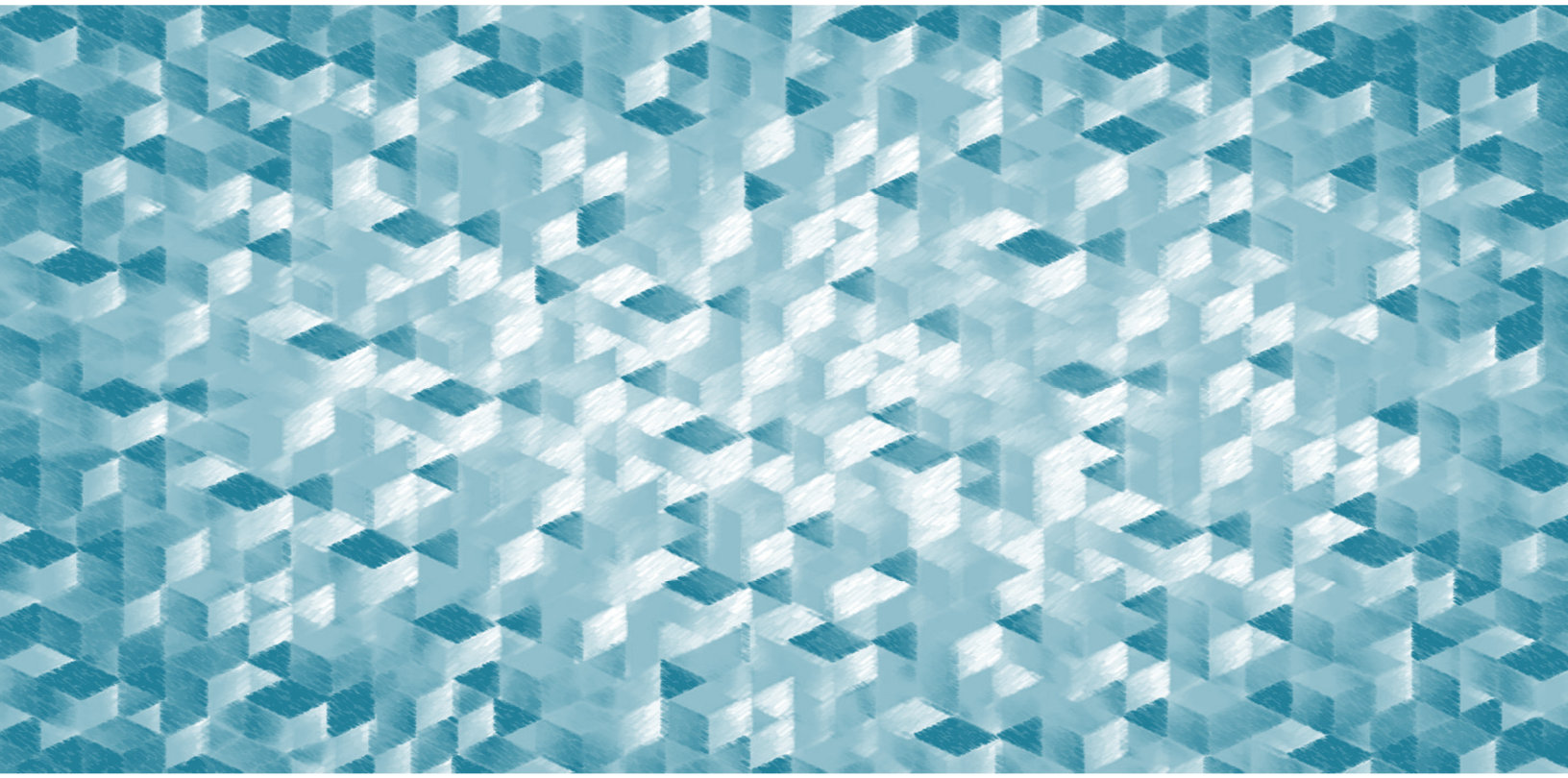


Cybersecurity

Critical Legal, Investigation and Risk Management Aspects

Contents

Cybersecurity

Cybersecurity: Critical Legal, Investigation & Risk Management Aspects

Lecturer/Trainer: Zaid Hamzah[1], Cybersecurity Lawyer, Practitioner and Author of "*E-Security Law and Strategy*" (Lexis Nexis, 2005)

COURSE OVERVIEW

Introduction

The phenomenal growth of the networked environment, the increase in the number of malicious cyberattacks and the heightened risk of cyberterrorism against critical information infrastructures (such as national power grid, transportation, health, banking and finance infrastructure) have made cybersecurity a critical national agenda. Cyberattacks harm national security and business interests and are considered as criminal acts in most jurisdictions. In dealing with cybersecurity attacks, understanding how the law and legal processes operate is a critical and unavoidable aspect. For example, when a cybercrime is committed, one needs to know whether the law has been broken and how digital evidence should be properly collected in accordance with the appropriate legal standards to ensure successful prosecution. The establishment of a robust legal risk management framework and prosecution regime to fight cybercrime is an essential building block at the organizational level. Enterprises, governments and other organizations needs to create a proactive and structured legal risk management framework to better manage cybersecurity risks and ensure cybersecurity resilience.

Objectives

This program will equip participants with the knowledge and skills to deal with cybersecurity attacks from the legal, investigative and risk management aspects. It will introduce the concepts and principles of computer crime laws and regulations, the investigative measures, methods and techniques which can be used to determine if a computer crime has been committed. The program will cover methods[2] to gather, preserve and present evidence of a computer crime and provide an overview of cybersecurity legal processes[3] from the time a cybercrime is committed through the prosecution process in court.

Who Should Attend

This program targets the following groups according to their needs and level of understanding:

---

[1] See biodata at Annex.

[2] The process of digital evidence collected is a technical process requiring technical tools and specialist know-how. This course will focus more on the legal and investigative aspects instead of the "hard" technical aspects.

[3] Note that cybersecurity laws are jurisdiction-specific and the laws vary from country to country. This course will provide both the general principles of cybersecurity law as well as specific national laws in the country in which this course is being taught.

1. Students in Tertiary Institutions
    a. Law students (university and diploma level students)
    b. ICT, Engineering and Business Students (university and diploma level students)
    c. Law lecturers (train-the-trainers) teaching law, IT, Engineering and Business

2. Legal Practitioner and Legal Advisors
    a. In-house counsels working in enterprises and government bodies
    b. Legal practitioners in private practice as well as Bar Councils or Law Societies
    c. Government lawyers (eg from Attorney-General Chambers)

3. IT and Business Professionals
    a. IT security professionals in particular and IT professionals in genera
    b. IT professionals taking the CISSP[4] examinations
    c. Business professionals

4. Law Enforcement Officers
   Those with responsibilities for cybersecurity investigations and enforcement including:
    a. Police
    b. Military; and
    c. Civil defence

5. Judicial officers (who deal with cybercrime cases), arbitrators and mediators

6. Policy makers responsible for cybersecurity policies

Learning Outcomes

By attending this program, participants will:

1. Learn the basic principles of cybersecurity laws and how to identify legal risk issues in the design, development and management of information security systems;
2. Know how to carry out investigation when a computer crime is suspected to have been committed including dealing with cross border legal and investigation issues and understanding criminal prosecution procedures.;
3. Understand how to manage digital evidence to ensure compliance with legal standards and requirements in court proceedings;
4. Understand key legal risk management principles and strategies that organizations should adopt as part of their overall information security management policy;
5. Learn how they can better deal with legal and regulatory compliance in information security arena against the context of the need to develop a robust governance, risk and compliance framework; and
6. Learn how to better operate in an international environment when cybercrimes take place across borders including how to enhance cooperation at the international level.

[4] Certified Information System Security Professional qualifications

Multi-disciplinary Approach

The program takes a practical and multi-disciplinary[5] approach focusing on key knowledge and skills that the participants would need in order to function more effectively in this high risk environment. This program does not only deal with law but practical investigation strategies and techniques. It contextualizes the teaching of cybersecurity legal concepts and principles against the larger context of strategic risk management. The program emphasises real world setting and uses actual cybercrime cases in its case studies. Given the fact that cybercrime are often carried out across borders, the program also takes a cross-border perspective, especially in the area of digital evidence management between enforcement agencies.

During the course itself, a *problem-based* approach will be taken depending on the learner's readiness. Under this problem-based approach, a problem will be set out initially and students are encouraged to find solutions under the guide of the trainer as part of the learning process.

Performance-based, Experiential, Adaptive & Agile Learning ("*PEbAAL*")

Depending on the readiness of the institutions or organizations supporting the professional development of course participants, learning programs can be organized adopting the Performance-based, Experiential, Adaptive and Agile Learning methodology ("*PEbAAL*"). This methodology seeks to enhance performance at the workplace or during site investigation when a cybercrime has taken place. The ultimate aim of the program for professionals is to boost the overall performance of the organization, for example, in countering cybercrimes. The *PEbAAL* approach is available for both the face to face training or tailored online courses.

Under the *PEbAAL* approach, participants will initially undergo a pre-test to evaluate their existing knowledge and skills. During the course, each learner will be evaluated individually and post course follow up can be developed to suit the needs of learners with different capacities and levels of readiness.

[5] Those without any foundation in ICT (info-communication technology) will be given a crash course on IT systems

COURSE OUTLINE

PART 1: INTRODUCTION TO CYBERSECURITY LAW & CYBERCRIME

Concepts and Principles

1. Nature of cybersecurity, computer misuse and cybercrime
    a. What is cybersecurity law? What is cybercrime?
    b. How does computer crimes differ from civil cases
    c. How computer crime law work
        i. Intent and authorization
        ii. Law of attempts
    d. Why cybercrime is hard to define and hard to prosecute
2. Types of criminal offences and civil wrongs
    a. Types of computer crimes
        i. Crimes against the computer or the IT systems (eg network intrusion, introduction of malware, botnets[6], denial of service, bandwidth theft)
        ii. Crimes using the computer or IT system
            1. Banking and other financial crimes including online fraud
            2. Identity theft and online fraud
            3. Cyberstalking and online harassment
            4. Cyberterrorism
            5. Child exploitation
        iii. Content-related offences[7] - separate from computer crimes
    b. Privacy breaches and violation of personal data
        i. Principles of personal data protection
    c. Online theft of intellectual property
3. Roles of criminal justice professionals in the criminal justice system

Anatomy of a Cybercrime

4. Basic elements of cybercrime offence
    a. Intention & Action – legal definition of hacking, denial of service attacks
    b. Offences against the confidentiality, integrity and availability of computer data and systems
    c. Basic Types of Cybercrimes
        i. Unauthorized access
        ii. Unauthorized modifications and damage to data
        iii. Unauthorized interceptions and obstructions
5. Examples of Statutory Provisions in Cybersecurity Laws[8]
    a. Singapore
    b. Malaysia
    c. USA

---

[6] A **botnet** (also known as a zombie army) is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet

[7] For example, pornography

[8] The course contents can be tailored to meet the local jurisdiction – this is done with the support of local lawyers in that market where Zaid Hamzah, the lead trainer, does not the competencies to teach.

6. Applying the Law
    a. How to determine applicable cybersecurity law
    b. Major factors complicating prosecution
    c. Difficulties in defining the crime
    d. Basic criminal justice theory

Cybercrime Investigation

1. The investigative process
    a. How does one investigate a computer[9] or IT crime?
    b. Planning the investigation
    c. Preparations needed
    d. Understanding the legal process in investigations
    e. Obtaining evidence of criminality
2. Role of law enforcement officers
    a. Defining areas of responsibilities
    b. Understanding private sector investigations
3. Jurisdictional Issues
    a. Determine jurisdiction
    b. Determining power and capacity
    c. Cross border aspects
4. What is the basic investigation methods and techniques to determine if a computer crime has been committed?
5. How should an investigation be carried out?
    a. Securing a computer incident or crime scene
    b. Search and Seizure
        i. Who can seize evidence
    c. Understanding concept and terms in search warrants
    d. Constitutional issues – the US example
    e. Search without warrants
    f. Seizure of digital evidence
    g. Compliance with the law of procedures
6. Crimes in private premises & businesses
    a. When should police investigators be involved?

[9] For learners without an understanding of computers and IT systems, a separate introduction can be arranged to teach such basic technical concepts.

PART 2: HANDLING DIGITAL EVIDENCE IN CYBERCRIME CASES

1. Overview of digital forensics and the law
2. Evidence in general
    a. Why collect evidence
    b. Identifying digital evidence
    c. Evidence collection options
    d. Types of Evidence
        i. Direct and indirect evidence
        ii. Hearsay evidence
3. Rules of Evidence
    a. Best evidence rule
    b. Admissibility of evidence
        i. Complying with rules of procedures
        ii. Examples from selected Evidence Act
4. Managing Evidence in general
    a. Volatile evidence
5. Methods to gather, preserve and present evidence of a computer crime
    a. Preserving the digital crime scene
        i. Role of first responders
        ii. Role of investigators
    b. Computer evidence processing steps
        i. Preserving digital evidence
        ii. Controlling contamination: The Chain of Custody
        iii. Storing digital evidence
        iv. Documenting evidence
            1. Evidence tagging and marking
            2. Evidence logs
            3. Documenting evidence analysis
            4. Documenting the chain of custody

PART 3: PROSECUTING IN THE COURTS

1. Prosecution of Criminal Offences
    a. Building the cybercrime case - the trial process
    b. What is electronic document discovery
    c. What does a public prosecutor do in a court room?
    d. Typical documents in criminal proceedings
2. Burden of Proof
    a. Concept of burden of proof - what is the burden of proof required?
    b. What does “beyond reasonable doubt” mean?
    c. What does “on balance of probabilities” mean
3. How does the defence lawyer carry out defence in cybercrime cases?
    a. Basic techniques
        i. Challenging the method of evidence collection
        ii. Challenging the qualifications of the evidence collector
        iii. Raising doubts – its importance in criminal prosecution
    b. Advanced techniques
    c. Legal challenges in cloud forensics
4. Understanding Rules of Procedures
5. Testifying in a cybercrime case
    a. Testifying as an evidentiary witness
    b. Testifying as an expert witness
    c. Giving direct testimony
    d. Cross-examination tactics
6. Issues in cross border computer crime

PART 4: COMPUTER MISUSE & CYBERSECURITY ACT, SINGAPORE

This module is designed specifically for IT security personnel, business executives and lawyers operating in Singapore[10]. The course contents are specific to Singapore law and the Singapore legal system. For learners who are not based in Singapore, they will be able to understand the Singapore approach and evaluate how such an approach may be adapted and/or adopted in their own jurisdiction.

1. Understanding the history of the Computer Misuse and Cybersecurity Act (CMCA)
2. How to interpret legislative provisions[11]
3. Overview of the CMCA and the relationship with Criminal Procedure Code and Evidence Act
4. Analysis of the provisions of the CMCA

	OFFENCES
Section 3	Unauthorised access to computer material
Section 4	Access with intent to commit or facilitate commission of offence
Section 5	Unauthorised modification of computer material
Section 6	Unauthorised use or interception of computer service
Section 7	Unauthorised obstruction of use of computer
Section 8	Unauthorised disclosure of access code
Section 9	Enhanced punishment for offences involving protected computers
Section 10	Abetments and attempts punishable as offences
	MISCELLANEOUS AND GENERAL
Section 11	Territorial scope of offences under this Act
Section 12	Jurisdiction of Courts
Section 12A	Composition of Offences
Section 13	Order for payment of compensation
Section 14	Saving for investigations by police and law enforcement officers
Section 15A	Cybersecurity measures and requirements
Section 16	Arrest by police without warrant

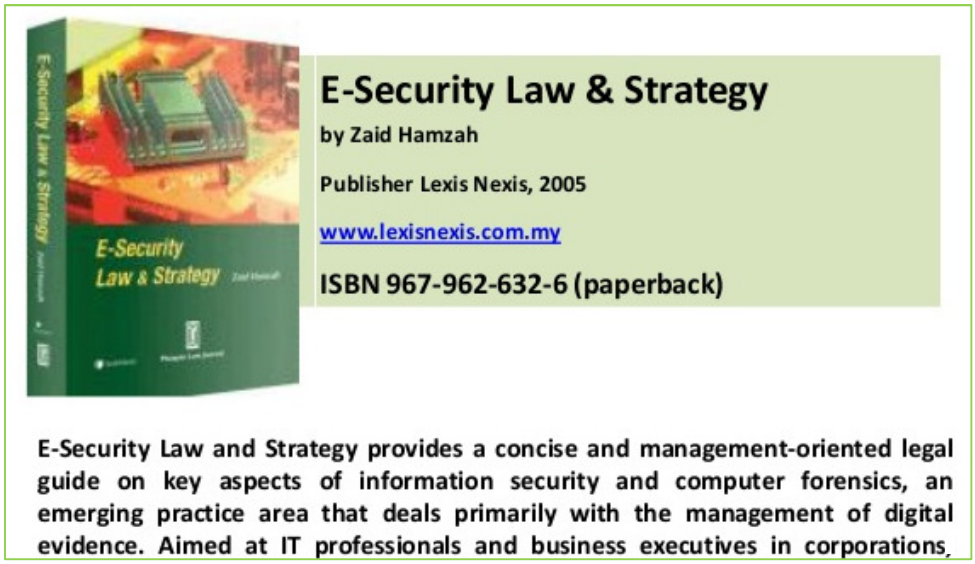
5. Electronic Evidence and Admissibility of "Computer Output"
    1. Traditional rules of admissibility
        a) Best evidence rule
        b) Authentication rule
        c) Rule against hearsay evidence
    2. Reliability of electronic records
6. Case Studies

[10] For learners operating in other jurisdictions, tailored courses will be organized to suit the local laws and regulations.
[11] For non-law students or non-lawyers, this section will go deeper so that these groups will have a stronger foundation.

BIODATA OF ZAID HAMZAH

A Strategic Counsel who specializes in Technology, Media & Telecoms including cybersecurity law and author of the book "E-Security Law and Strategy, Lexis Nexis 2005), Zaid has over 25 years of professional experience spanning the ICT[12]/media, e-security, e-commerce, intellectual property, technology commercialization, and intellectual capital sectors.

Presently CEO of the Law Society of Singapore, Zaid has deep experience in the legal aspects of cybersecurity and has taught Information Security Law as an Adjunct lecturer at Universiti Teknologi Malaysia. Working in collaboration with a Malaysian law firm, Zaid has designed and developed for a Manual for Digital Evidence for Cyber Security Malaysia[13]. He has also developed the online learning module for the CISSP[14] examination on Law, Investigation and Ethics for the Institute of Systems Science, National University of Singapore.



Zaid has previously served as Director at Microsoft Asia Pacific and as Chief Regulatory, Legal and Compliance Officer at Telekom Malaysia, the telecommunication incumbent in Malaysia. In 2014-2015, he was contracted by a joint-venture media company involving Singapore Telecommunications, Warner Brothers and Sony Pictures Entertainment. A commercially-oriented technology practitioner who specializes technology-based commercial transactions, Zaid has vast regional experience in South-east Asia (Singapore, Malaysia, Indonesia, Thailand and the Philippines) where he focused deeply on helping enterprises and research institutions improve

[12] InfoCommunication Technology
[13] CSM which was previously known as NISER is the Malaysian government agency responsible for cybersecurity policy
[14] Certified Information System Security Professional qualifications

business performance through business value creation and strategic legal risk management. Zaid was the founder and Managing Director of a start-up legal informatics company prior to becoming Director at Microsoft. Zaid has also practised as a regional lawyer with a major Singapore law firm and his own consulting practice. Zaid now runs his own consulting company, Intellectual Futures while he teaches part time at RMIT University program in Singapore.

Author of 9 books and passionate about teaching, Zaid is a Singaporean national who graduated with a law degree from the National University of Singapore. He completed his Masters in international relations at the Fletcher School of Law and Diplomacy, Tufts University, USA on a Fulbright scholarship.

end