

CYBER SECURITY LAW IN MALAYSIA

THEORY AND PRACTICE

MAHYUDDIN DAUD



SWEET & MAXWELL

Cyber Security Law in Malaysia

Theory and Practice

Mahyuddin Daud

PhD (IIUM), LLM (UiTM), LLB (Hons) (IIUM)

Associate Professor

Ahmad Ibrahim Kulliyyah of Laws

International Islamic University Malaysia



Published in 2025 by
Thomson Reuters Asia Sdn Bhd – 201801016202
E-03-GF, Ground Floor, Block E
Garden Shoppe, One City, Jalan USJ 25/1A
47650 Subang Jaya
Selangor Darul Ehsan, Malaysia

© Thomson Reuters Asia Sdn Bhd

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means or stored in any retrieval system of any nature without prior written permission, except for permitted fair dealing under the Copyright Act 1987. Application for permission for other use of copyright material including permission to reproduce extracts in other published works shall be made to the publisher. Full acknowledgement of the author, publisher and sources must be given.

The author has asserted his moral rights under the Copyright Act 1987, to be identified as the author of this publication.

ISBN 978-629-7700-64-9
ISBN 978-629-7700-65-6 (ProView eBook)

Printed by Yamagata (Malaysia) Sdn Bhd (219625-T)
Lot PT 1661, Nilai Industrial Estate, PO Box 9, 71809 Nilai, Negeri Sembilan

Contents

<i>Foreword</i>	v
<i>Preface</i>	vii
<i>Acknowledgements</i>	xiii
<i>About the Author</i>	xv
<i>List of Abbreviations</i>	xxiii
<i>Table of Cases</i>	xxv
<i>Table of Statutes</i>	xxvii

Chapter 1

Introduction to Cyber Security Law	1
Introduction	1
Cyber security vs cybercrime	1
Cyber-dependent crime vs cyber-enabled crime	6
What is the importance of cyber security in the modern Internet age?	7
Emergence of cyber threats	8
The first cyberattack?	9
Role of supranational bodies in cyber security	12
Cyber security in Malaysia	14
National Cyber Security Agency (NACSA)	15
Cyber security policies and strategies in Malaysia	16
Two decades of cyber law development: A revisit	19
Communications and Multimedia Act 1998 (Act 588)	19
Powers of the MCMC	21
Computer Crimes Act 1997 (Act 563)	22
Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (Act 613)	24
National Anti-Financial Crime Centre Act 2019 (Act 822)	25
Penal Code (Act 574)	25
Personal Data Protection Act 2010 (Act 709)	27
Electronic Commerce Act 2006 (Act 658)	28
Electronic Government Activities Act 2007 (Act 680)	29
National Security Council Act 2016 (Act 776)	29
Protected Areas and Protected Places Act 1959 (Act 298) (Revised 1983)	30
Financial Services Act 2013 (Act 758)	31
Islamic Financial Services Act 2013 (Act 759)	31
Conclusion	31

Chapter 2**Understanding the Cyber Security Act 2024..... 33**

Introduction	33
Background	33
Key principles and features	34
Extra-territorial application	34
Global nature of cyber threats	35
Cross-border collaboration/cyber diplomacy	35
Protection of national interests	35
Deterrence and legal framework.....	36
Harmonisation of standards	36
Application of the Cyber Security Act 2024	
to the government.....	38
Obligation of secrecy.....	43
Data security principle and cyber security	44
Disclosure of information to the Chief Executive	
of the NACSA.....	45
Criminal offences.....	47
Corporate liability for cyber security.....	58
Generally.....	58
Corporate liability under the Cyber Security Act 2024.....	61
Position on cyber security corporate liability in Australia	64
Conclusion	65

Chapter 3**Cyber Security Governance 67**

Introduction	67
Cyber security regulator in Malaysia	68
Establishment of the National Cyber Security Committee	
under the Cyber Security Act 2024	68
Role of the Chief Executive of the National Cyber	
Security Agency	71
National critical information infrastructure sector leads under	
the Cyber Security Act 2024	72
Overview.....	72
Responsibilities of national critical information	
infrastructure sector leads	75
National critical information infrastructure entity.....	79
Technical support.....	81
Overview.....	81
National Cyber Coordination and Command Centre (NC4).....	82
CyberSecurity Malaysia.....	84
Governance structure of cyber security lead agencies	
in other countries.....	86

Singapore	86
The United States	89
Australia	94
The European Union	95
Japan	97
China	103
The United Kingdom	106
Conclusion	109

Chapter 4

Cyber Security Ecosystem – Protecting National Critical Infrastructures

Introduction	111
National critical information infrastructure (NCII) in Malaysia	113
Designation of NCII	115
Duties and responsibilities of NCII entity	120
Duty to provide information relating to national critical information infrastructure	120
Duty to implement code of practice	121
Duty to conduct cyber security risk assessment and audit	122
Requirements under specific regulations	124
Interpretation of cyber security risks	125
Requirements for cyber security risk assessments and audits	125
Enforcement and compliance oversight	127
Duty to notify cyber security incident	127
Procedure relating to submission of details by authorised persons	130
Immediate notification via electronic means	131
Subsequent updates relating to cyber security incidents	131
Communication method in event of disruption to the National Cyber Coordination and Command Centre System	131
Cyber security exercise	132
Comparison with other countries on NCII obligations	134
Singapore	134
The European Union	140
Australia	145
The United States	147
China	148
Key concerns and criticisms	152
Data localisation requirements	152
Ambiguous provisions and government access	153
Increased compliance costs	154

The United Kingdom.....	156
Key duties of operators of essential services (OES).....	160
Identification and notification of OES status.....	160
Requirement for risk management and security measures.....	160
Incident notification and response.....	162
Ongoing monitoring and review.....	162
Cooperation with competent authorities	162
Penalties for non-compliance.....	163
Conclusion.....	163

Chapter 5

Responses to Cyber Security Incidents

Introduction	165
Meaning of cyber security incident and cyber security threat.....	167
Notification of a cyber security incident.....	168
Overview.....	168
Notification of incident.....	169
Submission of information (within six hours)	169
Supplementary information (within 14 days).....	170
Submission method	170
Role of the National Cyber Coordination and Command Centre (NC4).....	171
Analysis and comments.....	173
Investigation and enforcement	177
Regulatory procedures.....	177
Compounding of offences under the Cyber Security Act 2024.....	181
Procedure for compounding offences.....	181
Singapore approach.....	182
The United Kingdom approach	183
The United States approach.....	185
Conclusion.....	187

Chapter 6

Licensing of Cyber Security Service Providers.....

Introduction	189
Roles and responsibilities of cyber security service providers	189
Threat detection and prevention	189
Incident response.....	190
Vulnerability assessment and penetration testing	190
Security consulting and risk management.....	190
Security monitoring and analytics.....	191
Security awareness training	191
Managed security services	191

Licensing and certification scheme for cyber security	
service providers	192
Certified Cybersecurity Awareness Educator (CCAЕ).....	194
Certified Security Operation Centre Analyst (CSOCA).....	194
Certified Incident Handling and	
Network Security Analyst (CIHNSA).....	195
Certified Industrial Control System Security Analyst (CICSSA).....	195
Certified MyCC Evaluator (CME).....	195
Certified IoT Security Analyst (CISA).....	195
Certified Secure Web Application Developer (CSWAD).....	196
Certified Data Security Analyst (CDSA)	196
Certified Secure Application Professional (CSAP)	196
Certified Information Security Awareness Manager (CISAM).....	197
Certified Information Security Management System	
Auditor (CISMSA)	197
Certified Digital Forensic for First Responder (CDFFR).....	197
Certified Penetration Tester (CPT).....	197
Professional Business Continuity Management (BCLE-2000)	197
ISO/IEC 27001:2013 Information	
Security Management System (ISMS) – Lead Auditor	198
Licensing Framework under the Cyber Security Act 2024 and	
Regulations.....	198
Overview.....	198
Licensing procedures.....	200
Checklist for application of cyber security service	
provider licence (as required under Arahan Ketua	
Eksekutif No 2/CSA 2024).....	203
Cyber Security Service Providers Licensing Framework	
in Singapore	204
The European Union Certification Framework	207
Conclusion	209

Chapter 7

Cyber Security Act 2024 and Beyond: Challenges in Malaysia.....

Introduction	211
Cyber resilience.....	212
IoT and BYOD	213
NCII and beyond	214
Supply chain.....	216
Impact of artificial intelligence on cyber security.....	217
Obligation to notify.....	217
What is understood as significant incidents with regard	
to the major online entities.....	218

Espionage activities from state-sponsored threat actors and cybercriminals.....	218
Cyber diplomacy and cyberwarfare.....	220
Cybercrime and cyber security	221
Certification or licensing	222
Individual and Institutional	223
<i>Index</i>	225

Preface

On July 19, 2024, global IT disruptions sent shockwaves through critical sectors, underscoring the cyber security issues that plague the world. A CrowdStrike update caused Microsoft Windows to fail, impacting users worldwide, including those in Malaysia. While initially claimed as not a cyberattack, this disruption brought to light the vulnerabilities in critical sectors. It was only two weeks later that Microsoft confirmed that the outage was caused by a cyberattack, namely, a Distributed Denial of Service (“DDoS”) attack¹ and a failure to defend against it properly.²

Earlier, the company issued an apology for the incident. The DDoS lasted almost 10 hours and caused thousands of users to report issues with Microsoft services. Less than two weeks after a major global outage left around 8.5 million computers using Microsoft systems inaccessible, impacting healthcare and travel, after a flawed software update by cyber security firm CrowdStrike. Tony Fernandes, CEO of Capital A or formerly AirAsia was recorded to demand compensation against Microsoft for the said cyber security incident.³ However, there are no public records that can confirm whether AirAsia is seeking to litigate the matter.

The incident mentioned above is just one of many recent events that have deeply affected people around the world. Unfortunately, there is

-
- 1 Cloudflare, “How to Prevent DDoS Attacks | Methods and Tools”, Cloudflare (2024), available at <https://www.cloudflare.com/learning/ddos/how-to-prevent-ddos-attacks/> (accessed March 28, 2025). A distributed denial-of-service (DDoS) attack disrupts the operations of a server, service, or network by flooding it with unwanted Internet traffic. At their worst, these attacks can knock a website or entire network offline for extended periods of time.
 - 2 Graham Fraser João da Silva, “Microsoft Says Cyber-Attack Triggered Latest Outage”, *BBC News* (2024), available at <https://www.bbc.com/news/articles/c903e793w74o> (accessed March 28, 2025).
 - 3 Lionel Lim, “AirAsia’s Tony Fernandes Wants Microsoft Compensation for the CrowdStrike Outage: ‘If I Delay My Flight, You Would Come after Me for a Refund’”, *The Star Online* (2024), available at <https://www.thestar.com.my/tech/tech-news/2024/07/25/airasias-tony-fernandes-wants-microsoft-compensation-for-the-crowdstrike-outage-if-i-delay-my-flight-you-would-come-after-me-for-a-refund> (accessed March 28, 2025).

Index

Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (Act 613), [1.076]–[1.079]

Artificial intelligence (AI)
cyber security, impact on,
[7.012]–[7.014]

Australia

corporate liability for cyber security,
[2.069]–[2.074]

Corporations Act 2001 (Cth),
[2.062], [2.069]

director duties, breaches of,
[2.072]–[2.074]

enterprises, regulatory burden
for, [2.071]

overview, [2.069]–[2.070]

Privacy Act 1988 (Cth), [2.062]

cyber security governance structure
of, [3.082]–[3.087]

Security of Critical Infrastructure
Act 2018. *See* SECURITY OF CRITICAL
INFRASTRUCTURE ACT 2018

**Australian Cyber Security Centre
(ACSC), [3.082]–[3.087]**

**Bring your own device (BYOD),
[7.006]**

**Certified Cybersecurity Awareness
Educator (CCAIE), [6.020]**

**Certified Data Security Analyst
(CDSA), [6.027]**

**Certified Digital Forensic for First
Responder (CDFFR), [6.031]**

**Certified Incident Handling
and Network Security Analyst
(CIHNSA), [6.022]**

**Certified Industrial Control
System Security Analyst (CICSSA),
[6.023]**

**Certified Information Security
Awareness Manager (CISAM),
[6.029]**

**Certified Information Security
Management System Auditor
(CISMSA), [6.030]**

**Certified IoT Security Analyst
(CISA), [6.025]**

**Certified MyCC Evaluator (CME),
[6.024]**

**Certified Penetration Tester (CPT),
[6.032]**

**Certified Secure Application
Professional (CSAP), [6.028]**

**Certified Secure Web Application
Developer (CSWAD), [6.026]**

**Certified Security Operation Centre
Analyst (CSOCA), [6.021]**

China

cyber security governance structure
of, [3.112]–[3.121]

Cybersecurity Law. *See*
CYBERSECURITY LAW

CIRCIA 2022. *See* CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022 (US)

CISA. *See* CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Communications and Multimedia Act 1998 (Act 588), [1.061]–[1.067]

Computer Crimes Act 1997 (Act 563), [1.068]–[1.075]

Corporate liability for cyber security

Australia's position, [2.069]–[2.074]
 Corporations Act 2001 (Cth), [2.062]
 director duties, breaches of, [2.072]–[2.074]
 enterprises, regulatory burden for, [2.071]
 overview, [2.069]–[2.070]
 Privacy Act 1988 (Cth), [2.062]
 Business Corporations Act (Canada), [2.060]–[2.061]
 Civil and Commercial Code (Thailand), [2.063]
 Companies Act 2006 (UK), [2.058]
 corporate directors legal obligation, [2.060]–[2.063]
 directors' accountability, mismanagement of user data, [2.058]–[2.059]
 Federal Data Protection Act (Germany), [2.062]
 Federal Office of Information Security Act (Germany), [2.062]
 generally, [2.057]

Critical information infrastructure operators

conduct annual security assessments, [4.150]
 Cybersecurity Law (China), [4.146]
 data localisation requirements, [4.149]
 data protection requirements, violations of, [4.154]

Critical information infrastructure operators (cont)

definitions of key terms, [4.155]
 early warning systems, creation of, [4.151]
 general network operators, applied to, [4.147]
 network security monitoring, creation of, [4.151]
 obligations for, [4.146]
 robust legal structure, [4.156]
 security obligations, penalties for non-compliance, [4.153]
 significant risk or emergency, government measures, [4.152]

CSA 2024. *See* CYBER SECURITY ACT 2024

Cyberattack

Advanced Research Projects Agency Network (ARPANET), [1.027]
 computer passwords, [1.030]
 Creeper virus, [1.029]
 financial institution, hackers attack on, [1.032]–[1.037]
 financial market information, stealing of, [1.028]
 Kevin Mitnick, first cybercriminal, [1.032]
 RABBITS virus, [1.031]
 ransomware attack, [1.036]
 Rene Carmille, first ethical hacker, [1.028]

Cyber-dependent crime

defined, [1.016]
 International Criminal Police Organization (Interpol), [1.018]–[1.019]

Cyber Emergency Response (Cyber999), [3.052]

Cyber-enabled crime

defined, [1.017]
 International Criminal Police Organization (Interpol), [1.018]–[1.019]

Cyber incidents

obligation to notify authorities, [7.015]

Cyber Incident Reporting for Critical Infrastructure Act of 2022 (US)

Cyber Incident Reporting Council, role of, [5.084]
 cyber security incidents, framework for managing, [5.077]–[5.078]
 Cybersecurity and Infrastructure Security Agency (CISA)
 information shared, critical protections for, [4.136]
 receive, analyse, and disseminate information, to, [4.135]
 reporting requirements, failure to comply with, [4.137]
 roles of, [4.134]
 incident reports, [5.079]
 legal protections for entities, [5.082]
 overview, [4.131]
 ransomware payment reporting requirements, [4.133]
 reporting framework, [5.085]
 risk management and mitigation strategies, [5.081]
 significant cyber incidents, reporting of, [4.132]
 threat intelligence and incident data, sharing of, [5.080]

Cyber resilience

Australia's security initiative, [7.003]
 bring your own device (BYOD), [7.006]
 critical sectors, focus on, [7.008]
 essential sectors, identification of, [7.007]
 European Union (EU)
 Cyber Resilience Act, [7.005]
 proposal for, [7.002]
 Internet of Things (IoT), [7.006]
 low-revenue and higher revenue organisations gaps, [7.004]
 overview, [7.001]–[7.003]
 risk management framework, establishment of, [7.004]

Cyber resilience (*cont*)

Singapore's essential services, [7.010]
 United Nations (UN) Open Ended Working Group, [7.009]
 UN Norms, [7.017]–[7.019]

Cybersecurity Act 2018

(Singapore), [1.004], [3.055]–[3.064]
 computer or computer system, evaluation of, [4.024]
 critical information infrastructure (CII)
 Commissioner's role, [4.086]–[4.089]
 duties of owner, [4.090]–[4.096]
 essential service, defined, [4.085]
 maintenance of, [4.083]
 national cyber security, legal framework, [4.083]
 regulations, [4.097]–[4.102]
 responsibilities of, [4.084]
 criticalness of entity, [4.023]
 cyber security incidents, approach to, [5.064]–[5.068]
 dual penalty regime, [2.053]
 encourage compliance, [2.054]–[2.055]
 how entity qualifies, criteria for, [4.022]

Cyber Security Act 2024, [1.002]

Chief Executive of NACSA, disclosure of information to, [2.042]–[2.047]
 corporate liability for cyber security.
 See CORPORATE LIABILITY FOR CYBER SECURITY
 corporate liability under
 directors' actions as defence, [2.067]
 individuals in management roles, [2.064]–[2.067]
 criminal offences, [2.048]–[2.056]
 data security principle and cyber security, [2.035]–[2.041]
 draft of, [2.001]
 duties and responsibilities, failure to carry out, [2.056]

Cyber Security Act 2024 (cont)

government, application to, [2.021]–[2.032]

licensing framework under

- applicants, conditions for, [6.038]
- application, electronic submission of, [6.039]
- conditions, modification or revocation of, [6.041]
- engagement, maintenance of records, [6.042]
- licence, renewal of, [6.040]
- licence, suspension or revocation of, [6.043]
- licence, transfer of, [6.044]
- overview, [6.035]–[6.036]
- service providers, requirement of valid licence, [6.037]

National Critical Information Infrastructure (NCII), [2.001]

- governance structure, managing of, [2.003]
- non-compliance, cases of, [2.005]
- risk assessments and audits, [2.004]
- sector leads, [3.017]–[3.032]

National Cyber Security Committee, establishment of, [3.007]–[3.010]

non-compliance, penalties for, [2.052]

obligation of secrecy, [2.033]–[2.034]

offences and punishments, list of, [2.051]

overview, [2.075]–[2.078]

principles and features

- cross-border collaboration/cyber diplomacy, [2.009]
- cyber threats, global nature of, [2.008]
- deterrence and legal framework, [2.011]
- extra-territorial application, [2.006]–[2.007]
- harmonisation of standards, [2.012]–[2.020]
- national interests, protection of, [2.010]

protection, proper level of, [2.002]

Singapore's Cybersecurity Act 2018, [2.053]–[2.056]

Cyber security certification

Certified Cybersecurity Awareness Educator (CCAEE), [6.020]

Certified Data Security Analyst (CDSA), [6.027]

Certified Digital Forensic for First Responder (CDFFR), [6.031]

Certified Incident Handling and Network Security Analyst (CIHNSA), [6.022]

Certified Industrial Control System Security Analyst (CICSSA), [6.023]

Certified Information Security Awareness Manager (CISAM), [6.029]

Certified Information Security Management System Auditor (CISMSA), [6.030]

Certified IoT Security Analyst (CISA), [6.025]

Certified MyCC Evaluator (CME), [6.024]

Certified Penetration Tester (CPT), [6.032]

Certified Secure Application Professional (CSAP), [6.028]

Certified Secure Web Application Developer (CSWAD), [6.026]

Certified Security Operation Centre Analyst (CSOCA), [6.021]

ISO/IEC 27001:2013 Information Security Management System (ISMS), [6.034]

Professional Business Continuity Management (BCLE-2000), [6.033]

Cybersecurity (Critical Information Infrastructure) Regulations 2018, [4.097]–[4.102]**Cyber security exercise**

Chief Executive of NACSA

- directions, failure to comply with, [4.081]
- NCII entity, assess readiness of, [4.079]
- NCII entity, directions to test preparedness, [4.080]

managing cyber risks, improvement in, [4.077]

Cyber security exercise (cont)

- NCII entities, importance of readiness, [4.082]
- NCII entities preparedness, evaluation of, [4.078]
- structured activity, cyber incidents response strategies, [4.075]
- type and objectives, [4.076]

Cyber security governance

- Chief Executive of NACSA, roles of, [3.137]
- comparative analyses, regulatory and enforcement powers, [3.138]
- CyberSecurity Malaysia, [3.139]
- National Cyber Security Agency (NACSA)
 - Chief Executive, roles of, [3.137]
 - overview, [3.004]
- National Cyber Security Committee, establishment of, [3.007]–[3.010]
- NCII entities, [3.140]–[3.141]
- operations, institutional organisation and coordination of, [3.001], [3.003]
- other countries, governance structure of
 - Australia, [3.082]–[3.087]
 - China, [3.112]–[3.121]
 - European Union, [3.088]–[3.091]
 - Japan, [3.092]–[3.111]
 - Singapore, [3.055]–[3.064]
 - United Kingdom, [3.122]–[3.135]
 - United States, [3.065]–[3.081]
- overview, [3.136]
- regulator, [3.005]–[3.006]
- structure and collaboration framework, [3.002]
- technical support
 - CyberSecurity Malaysia, [3.046]–[3.054]
 - National Cyber Coordination and Command Centre (NC4), [3.042]–[3.045]
 - overview, [3.036]–[3.041]

Cyber security incidents, responses to

- compounding of offences overview, [5.058]–[5.059]

Cyber security incidents, responses to (cont)

- compounding of offences (cont)
 - procedure for, [5.060]–[5.063]
- cyber security threat, compared, [5.011]–[5.012]
- defined, [5.008]–[5.012]
- investigation and enforcement
 - compounding of offences, [5.058]–[5.063]
 - regulatory procedures, [5.045]–[5.057]
- National Cyber Coordination and Command Centre (NC4), role of, [5.023]–[5.031]
 - during crisis, [5.025]
 - overview, [5.023]
 - during peace, [5.024]
- notification of
 - analysis and comments, [5.032]–[5.044]
 - information on, [5.017]–[5.018]
 - NC4, role of, [5.023]–[5.031]
 - overview, [5.013]–[5.016]
 - submission method, [5.022]
 - submission of information (within six hours), [5.019]
 - supplementary information (within 14 days), [5.020]–[5.021]
- overview, [5.001]–[5.007]
- Russia-Ukrainian War, [5.001]–[5.003]
- Singapore approach, [5.064]–[5.068]
- United Kingdom approach, [5.069]–[5.076]
- United States approach, [5.077]–[5.085]

Cybersecurity and Infrastructure Security Agency (CISA),

- [3.065]–[3.081]
- information shared, critical protections for, [4.136]
- receive, analyse, and disseminate information, to, [4.135]
- reporting requirements, failure to comply with, [4.137]
- roles of, [4.134]

Cyber security law

- artificial intelligence, impact of cloud-based services, [7.014]

Cyber security law (cont)

- artificial intelligence, impact of (cont)
 - leverage on, [7.013]
 - overview, [7.012]
- bring your own device (BYOD), [7.006]
- certification or licensing, [7.025]–[7.027]
- confidentiality, integrity and availability (CIA) triad, [1.007]–[1.008]
- cyberattack
 - Advanced Research Projects Agency Network (ARPANET), [1.027]
 - computer passwords, [1.030]
 - Creeper virus, [1.029]
 - financial institution, hackers attack on, [1.032]–[1.037]
 - financial market information, stealing of, [1.028]
 - Kevin Mitnick, first cybercriminal, [1.032]
 - RABBITS Virus, [1.031]
 - ransomware attack, [1.036]
 - Rene Carmille, first ethical hacker, [1.028]
- cybercrime and cyber security, [7.023]–[7.024]
- cyber-dependent crime vs cyber-enabled crime, [1.015]–[1.020]
- cyber diplomacy and cyberwarfare, [7.020]–[7.022]
- cyber incidents, [1.012]–[1.014]
- cyber incidents, obligation to notify authorities, [7.015]
- cyber resilience. *See* CYBER RESILIENCE
- cyber security
 - cybercrime and, defined, [1.010]
 - incident, [1.009]
- cyber security regulations, prevent cyberattacks, [1.011]
- cyber threats, emergence of, [1.025]–[1.026]
- definition, [1.003]–[1.007]
- free information sharing between organisations, [7.016]
- individual and institutional, [7.028]
- International Telecommunication Union defines, [1.003]

Cyber security law (cont)

- Internet of Things (IoT), [7.006]
- Malaysia, in, [1.045]–[1.048]
 - cyber law development, [1.060]–[1.104]
 - cyber security policies and strategies, [1.052]–[1.059]
 - National Cyber Security Agency (NACSA), [1.049]–[1.051]
- modern Internet age, importance of cyber security
 - cloud computing, [1.024]
 - computers and digital devices, destruction of, [1.022]
 - ethical hacking, concept of, [1.023]
 - overview, [1.021]
 - sensitive information and identity theft, disclosure of, [1.022]
- overview, [1.001]–[1.002]
- Singapore's Cybersecurity Act 2018, [1.004]
- supranational bodies, role of, [1.038]–[1.044]
 - Budapest Convention on Cybercrime, [1.038]–[1.040]
 - General Data Protection Regulation (GDPR), [1.043]
 - international entities and organisations, [1.042]
 - United Nations Convention against Cybercrime, [1.044]
 - United Nations Security Council, [1.041]
- UN Norms, [7.017]–[7.019]

Cybersecurity Law (China)

- ambiguous provisions and government access, [4.160]–[4.161]
- application of, [4.139]
- critical information infrastructure operators
 - conduct annual security assessments, [4.150]
- Cybersecurity Law (China), [4.146]
- data localisation requirements, [4.149]
- data protection requirements, violations of, [4.154]
- definitions of key terms, [4.155]

Cybersecurity Law (China) (cont)

- critical information infrastructure operators (cont)
 - early warning systems, creation of, [4.151]
 - general network operators, applied to, [4.147]
 - network security monitoring, creation of, [4.151]
 - obligations for, [4.146]
 - robust legal structure, [4.156]
 - security obligations, penalties for non-compliance, [4.153]
 - significant risk or emergency, government measures, [4.152]
- cyber security awareness and education, campaigns on, [4.142]
- data localisation, requirements of, [4.158]–[4.159]
- governance, structure of, [3.112]–[3.121]
- increased compliance costs, foreign firms, [4.162]–[4.168]
- network operators, [4.143]–[4.145]
- network security and informatisation, development of, [4.140]
- network security strategy, development of, [4.141]
- overview, [4.138]
- tiered system of network security protections, [4.143]
- users real identities, verification of, [4.144]

CyberSecurity Malaysia, [3.046]–[3.054], [3.139]

- Cyber Emergency Response (Cyber999), [3.052]
- digital forensics, [3.053]
- mission, focus of, [3.047]
- objectives, [3.048]
- overview, [3.046]
- security assurance, [3.053]
- security management and best practices, [3.053]
- services provided by, [3.051]
- training and outreach, [3.053]

Cyber security service providers

- checklist for licence application, [6.054]

Cyber security service providers (cont)

- European Union certification framework, [6.066]–[6.075]
- licence, procedures for, [6.045]–[6.054]
- licensing and certification, scheme for
 - certifications, descriptions for, [6.019]–[6.034]
 - competency requirements, standards of, [6.016]
 - information asymmetry, problem of, [6.017]
 - licensing framework, objective of, [6.013]–[6.018]
- Malaysian Communications and Multimedia Commission (MCMC), [6.014]
- overview, [6.011]–[6.012]
- quality of service, [6.015]
- licensing framework
 - applicants, conditions for, [6.038]
 - application, electronic submission of, [6.039]
 - conditions, modification or revocation of, [6.041]
 - engagement, maintenance of records, [6.042]
 - licence, renewal of, [6.040]
 - licence, suspension or revocation of, [6.043]
 - licence, transfer of, [6.044]
 - overview, [6.035]–[6.036]
 - service providers, requirement of valid licence, [6.037]
 - Singapore, in, [6.055]–[6.065]
- overview, [6.001]–[6.002], [6.076]–[6.079]
- roles and responsibilities of
 - incident response, [6.004]
 - managed security services, [6.009]–[6.010]
 - security awareness training, [6.008]
 - security consulting and risk management, [6.006]
 - security monitoring and analytics, [6.007]

Cyber security service providers (*cont*)

roles and responsibilities of (*cont*)
 threat detection and prevention,
 [6.003]
 vulnerability assessment and
 penetration testing, [6.005]

Cyber security threat

cyber security incident, compared,
 [5.011]–[5.012]
 defined, [5.010]

Cyberwarfare, [7.017]**Digital forensics**, [3.053]**Duty of NCII entities to conduct cyber security risk assessment and audit**, [4.038]–[4.044]**Duty of NCII entities to implement code of practice**, [4.030]–[4.037]**Duty of NCII entities to notify cyber security incident**, [4.056]–[4.064]**Duty of NCII entities to provide information**, [4.027]–[4.029]**Electronic Commerce Act 2006 (Act 658)**, [1.091]–[1.092]**Electronic Government Activities Act 2007 (Act 680)**, [1.093]**ENISA**. *See* EUROPEAN UNION AGENCY FOR CYBERSECURITY**Ethical hacking, concept of**, [1.023]**European Union (EU)**

certification framework,
 [6.066]–[6.075]
 cyber resilience
 Cyber Resilience Act, [7.005]
 Internet of Things (IoT) and bring
 your own device (BYOD), [7.006]

European Union (EU) (*cont*)

cyber resilience (*cont*)
 proposal for, [7.002]
 cyber security, governance structure
 of, [3.088]–[3.091]
 Cybersecurity Act (formally
 Regulation (EU) 2019/881), [4.103],
 [4.122], [7.002]
 European Union Agency for
 Cybersecurity. *See* EUROPEAN UNION
 AGENCY FOR CYBERSECURITY

European Union Agency for Cybersecurity, [3.088]–[3.091]

business environment, [4.113]
 certification framework, [4.105]
 critical infrastructure operators
 critical infrastructures, strengthen
 security of, [4.120]
 cyber security-certified products
 and services, adoption of, [4.119]
 essential services, security and
 resilience of, [4.121]
 overview, [4.116]
 reporting obligation to, [4.118]
 responsibilities of, [4.117]
 risk management, [4.118]
 security-by-design and security-
 by-default, principles of, [4.120]
 critical sectors, protection of, [4.108]
 cyber hygiene, [4.109]
 cyber security certification system,
 [4.110]
 EU member states, coordination
 between, [4.107]
 information and communication
 technologies (ICT), importance of,
 [4.103]
 public procurement, use of cyber
 security certification in, [4.115]
 responsibilities of, [4.104]
 security authorities, peer review
 system for, [4.114]
 security-by-design approach, [4.106]
 support innovation, goal to, [4.111]
 transparency and efficiency in
 operations, [4.112]

Financial Services Act 2013 (Act 758), [1.101]–[1.102]

General Data Protection Regulation (GDPR), [1.043], [4.177]

Internet of Things (IoT), [7.006]

Islamic Financial Services Act 2013 (Act 759), [1.103]–[1.104]

ISO/IEC 27001:2013 Information Security Management System (ISMS), [6.034]

Japan

cyber security, governance structure of, [3.092]–[3.111]

Malaysia

cyber law development, [1.060]–[1.104]
 Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (Act 613), [1.076]–[1.079]
 Communications and Multimedia Act 1998 (Act 588), [1.061]–[1.067]
 Computer Crimes Act 1997 (Act 563), [1.068]–[1.075]
 Electronic Commerce Act 2006 (Act 658), [1.091]–[1.092]
 Electronic Government Activities Act 2007 (Act 680), [1.093]
 Financial Services Act 2013 (Act 758), [1.101]–[1.102]
 Islamic Financial Services Act 2013 (Act 759), [1.103]–[1.104]
 National Anti-Financial Crime Centre Act 2019 (Act 822), [1.080]–[1.081]
 National Security Council Act 2016 (Act 776), [1.094]–[1.098]
 overview, [1.060]
 Penal Code (Act 574), [1.082]–[1.087]
 Personal Data Protection Act 2010 (Act 709), [1.088]–[1.090]
 Protected Areas and Protected Places Act 1959 (Act 298) (Revised 1983), [1.099]–[1.100]

Malaysia (cont)

cyber security, [1.045]–[1.048]
 CyberSecurity Malaysia. *See* CYBERSECURITY MALAYSIA
 cyber security policies and strategies
 government service delivery, security and dependability of, [1.059]
 Malaysia Cyber Security Strategy 2020–2024 (MCSS), [1.056]–[1.058]
 National Cyber Security Policy 2006 (NCSP), [1.054]–[1.055]
 overview, [1.052]
 safe cyber security framework, importance of, [1.053]
 National Critical Information Infrastructures. *See* NATIONAL CRITICAL INFORMATION INFRASTRUCTURES
 National Cyber Security Agency (NACSA), [1.049]–[1.051]
 overview, [1.105]–[1.107]

National Anti-Financial Crime Centre Act 2019 (Act 822), [1.080]–[1.081]

National Critical Information Infrastructure (NCII), [2.001]

authorised persons, procedure to submit details, [4.065]–[4.067]
 Chief Executive, authority of, [3.026]–[3.027]
 cyber security incidents, subsequent updates relating to, [4.069]
 cyber security risks
 assessments and audits, requirements for, [4.050]–[4.053]
 enforcement and compliance oversight, [4.054]–[4.055]
 interpretation of, [4.049]
 defined, [3.017]
 designating computers or computer systems, [4.025]
 designation letters, [3.028]–[3.029]

National Critical Information Infrastructure (NCII) (*cont*)

designation of
 classified entity, [4.014]
 overview, [4.013]
 PETRONAS, [4.020]
 relevant information by entity,
 disclosure of, [4.017]
 entities, [3.140]–[3.141]
 cyber threats, protection from,
 [3.035]
 defined, [3.018], [3.034]
 duties and responsibilities
 of conduct cyber security risk
 assessment and audit, duty
 to, [4.038]–[4.044]
 cyber security exercise,
 [4.075]–[4.082]
 implement code of practice,
 duty to, [4.030]–[4.037]
 notify cyber security incident,
 duty to, [4.056]–[4.064]
 overview, [4.026]
 provide information about
 systems, duty to, [4.027]–[4.029]
 requirements under specific
 regulations, [4.045]–[4.048]
 infrastructures, [3.033]
 revocation of NCII entity
 designation, process for, [3.025]
 essential sectors, identification of,
 [7.007]–[7.010]
 facilities, examples of, [4.003]
 government entity, definition of,
 [4.019]
 governments and organisations, key
 concern for, [4.002]
 governance structure, managing of,
 [2.003]
 immediate notification *via* electronic
 means, [4.068]
 Malaysia, in, [4.005]–[4.012]
 common threats, [4.011]
 computer, defined, [4.006]
 computer system, defined, [4.007]
 critical services, management of,
 [4.008]
 defined, [4.005]
 information and communication
 technologies, [4.009]

National Critical Information Infrastructure (NCII) (*cont*)

Malaysia, in (*cont*)
 other critical infrastructures,
 [4.010]
 strategies and regulations,
 [4.012]
 National Cyber Coordination
 and Command Centre System,
 communication method in event
 of disruption to, [4.070]–[4.074]
 National Cyber Security Baseline,
 [4.047]–[4.048]
 non-compliance, cases of,
 [2.005]
 other countries, comparison with,
 [4.075]–[4.082]
 Australia, [4.123]–[4.130]
 China, [4.138]–[4.168]
 European Union, [4.103]–[4.122]
 Singapore, [4.083]–[4.102]
 United Kingdom, [4.169]–[4.196]
 United States, [4.131]–[4.137]
 overview, [4.001], [4.197]–[4.201]
 risk assessments and audits,
 [2.004]
 sector leads, [3.017]–[3.032]
 appointed under section 15,
 [3.020]
 appointment of, [3.019], [3.024]
 Codes of Practice, [3.030]–[3.031]
 essential areas, encompassing of,
 [3.023]
 key functions, [3.021]–[3.022]
 notify Chief Executive of NACSA,
 duty to, [4.021]
 responsibilities of, [3.021]–[3.032]
 self-assessment, [4.047], [4.048]
 supply chain's role, [7.011]

National Cyber Coordination and Command Centre (NC4)

Chief Executive, statutory role in
 establishing, [3.042]
 crisis management purposes,
 [3.043]
 role of during, [5.023]–[5.031]
 crisis, [3.045], [5.025]
 overview, [5.023]
 peace, [3.044], [5.024]

National Cyber Security Agency (NACSA)

Chief Executive

roles of, [3.011]–[3.016], [3.137]

disclosure of information to, [2.042]–[2.047]

cyber security regulator, [3.005]–[3.006]

National Cyber Security Committee

establishment of, [3.008]

functions of, [3.009]–[3.010]

overview, [3.007]

National Security Council Act 2016 (Act 776), [1.094]–[1.098]

NCII. See NATIONAL CRITICAL INFORMATION INFRASTRUCTURES

NC4. See NATIONAL CYBER COORDINATION AND COMMAND CENTRE

Network and Information Systems Regulations 2018, [3.122]–[3.135]

designated competent authorities, responsibility of, [4.180]

General Data Protection Regulation (GDPR), [4.177]

groups of organisations, application on, [4.172]

Information Commissioner's Office (ICO), role of, [4.174], [4.181]–[4.183]

operators of essential services (OES) application on, [4.178]

cooperation with competent authorities, [4.195]

incident notification and response, [4.192]–[4.193]

non-compliance, penalties for, [4.196]

obligations for entities, [4.179], [4.184]

ongoing monitoring and review, [4.194]

risk management and security measures, requirement for, [4.187]–[4.191]

Network and Information Systems Regulations 2018 (cont)

operators of essential

services (OES) (cont)

status, identification and

notification of, [4.185]–[4.186]

overview, [4.169]–[4.171]

relevant digital service providers (RDSPs)

defined, [4.173]

Information Commissioner's Office (ICO), role of, [4.174]

obligations, [4.179]

small and micro businesses,

exemption for, [4.175]–[4.176]

Penal Code (Act 574),

[1.082]–[1.087]

Personal Data Protection Act 2010 (Act 709), [1.088]–[1.090]

Professional Business Continuity Management (BCLE-2000), [6.033]

Protected Areas and Protected Places Act 1959 (Act 298)

(Revised 1983), [1.099]–[1.100]

Security of Critical Infrastructure Act 2018

critical infrastructure assets

defined, [4.126]

entities responsible for, [4.127]

prompt reporting of incidents, [4.128]

critical information

infrastructure (CII)

Commissioner's role, [4.086]–[4.089]

duties of owner, [4.090]–[4.096]

essential service, defined, [4.085]

maintenance of, [4.083]

national cyber security, legal framework, [4.083]

regulations, [4.097]–[4.102]

responsibilities of, [4.084]

cyber security service providers

licensing framework, [6.055]–[6.065]

Security of Critical Infrastructure**Act 2018** (*cont*)

manage risks to critical
infrastructure, [4.125]

Minister and Secretary, significant
powers to, [4.129]

overview, [4.123]–[4.124], [4.130]

Singapore

Cybersecurity Act 2018. *See*

CYBERSECURITY ACT 2018 (SINGAPORE)

cyber security governance structure
of, [3.055]–[3.064]

United Kingdom

corporate liability for cyber security,
[2.058]

United Kingdom (*cont*)

cyber security, governance structure
of, [3.122]–[3.135]

cyber security incidents, responses
to, [5.069]–[5.076]

Network and Information Systems
Regulations 2018. *See* NETWORK AND
INFORMATION SYSTEMS REGULATIONS 2018

United States

Cyber Incident Reporting for Critical
Infrastructure Act of 2022. *See*

CYBER INCIDENT REPORTING FOR CRITICAL
INFRASTRUCTURE ACT OF 2022 (US)

cyber security, governance structure
of, [3.065]–[3.081]

cyber security incidents, responses
to, [5.077]–[5.085]

Today's life is shaped by the cyber sphere in many ways, whether through emails, social media, video conferencing, data exchange, cloud storage, digital finance, or internet searches. Cyber risks and security breaches are prevalent – a global IT disruption from a cyber attack can bring the entire business world to a halt; scams, hacking, and phishing lead to substantial losses.

In light of these risks and threats, heightened vigilance, keen awareness, and strong cyber security measures are vital to protect all sectors of society. This book examines Malaysia's legislative response to growing digital threats. It provides a clear understanding of the newly implemented Cyber Security Act 2024 (CSA 2024), analyses cyber security governance, and explores the safeguarding of national critical information infrastructures within the cyber security ecosystem. Various frameworks and best practices for handling cyber security incidents are reviewed. The book also discusses the licensing of cyber security service providers under the CSA 2024, offering a comprehensive appreciation of how the regulations work to improve consumer protection, elevate industry standards, and reinforce Malaysia's cyber security ecosystem.

This book will be an essential guide for legal professionals, IT security experts, compliance officers, business owners, and students navigating the complexities of cyber security law.

Key Features

- Extensive coverage of the entire cyber security landscape and its regulatory framework.
- In-depth explanation of the functioning of the CSA 2024.
- Thorough analysis of cyber security governance and the responsibilities of NACSA (National Cyber Security Agency).
- Examination of how cyber security supports national security by protecting national critical information infrastructures.
- Practical insights into strategies to respond to cyber security incidents.
- Overview of the National Cyber Coordination and Command Centre (NC4) established under the CSA 2024.
- Summary of the licensing system for cyber security service providers.

ISBN 978-629-7700-64-9

