

CYBER SECURITY

EVERYONE SHOULD

ALERT





CYBER SECURITY

EVERYONE SHOULD

ALERT



NIK ZULKARNAEN KHIDZIR
WAN NURULASIAH WAN MUSTAPA
RAZWAN MOKHTAR

Copyright UMK PRESS, 2023

All rights reserved. No part of this publication may be reproduced, stored in production transmitted in any form, whether electronic, mechanical, photocopying, recording or otherwise, without having permission from the UMK Press.



Cataloguing-in-Publication Data

Perpustakaan Negara Malaysia

A catalogue record for this book is available
from the National Library of Malaysia

ISBN 978-967-0021-79-9

Executive Producer: Azman Hashim. Copy Editor: Amirul Firdaus Zilah,
Raihana Sulaiman. Acquisition Editor: Nur Fatimah Pahazri.
Concept & Typesetting: Fatinah Ilias. Proof Reader: Zaliha Noor
Technical Assistant: Mohd Suhairi Mohamad.

Published by:

UMK Press

Universiti Malaysia Kelantan

Office of Library and Knowledge Management

16300 Bachok, Kelantan

(Member of Malaysian Scholarly Publishing Council (MAPIM))

(Member of Malaysian Book Publishers Association (MABOPA))

Membership Number : 201903)

Printed by:

Visual Print Sdn Bhd

No.47, 47-1, Jalan Damai Raya 1,

Alam Damai, Cheras 56000

Kuala Lumpur

TABLE CONTENTS

List of Figures	ix
List of Abbreviations	xi
Preface	xiii
Book Overview	xv

CHAPTER 1 INTRODUCTION

What is Cyber Security?	1
What Happen When the Security Fails?	1
What is Weakest Link of Cyber Security?	3
A World Without Cyber Security	4

CHAPTER 2 CYBER THREATS IN THE INFORMATION AGE

The Nature of Threats	7
The Internet of Things (IoT)	9
Botnet Armies	12
When Security is an Afterthought	14
Autonomous Systems	14
Driverless Cars and Transport	15
ATMs and Point of Sale	16
Wearables	18
Cyberwarfare	19
Automated Attacks	19
Cyberattacks on Infrastructure	20
Data Manipulation	21
Backdoors	21
Cloud Concern	22
Virtualized Threats	23
Industry and Individual	24
Ransomware and Crypto Ware	24
Identity Theft	25

CHAPTER 3 CYBERSPACE AND DIGITAL TECHNOLOGY

The 100% Secure Computer	28
Opportunities	29
The Data-Driven Economy	29
Technology as Wealth Creation	29
Cybersecurity as Job Growth	30
Leveraging Technology Talent	31
Challenges	31
Leadership	32
Collaboration	32

CHAPTER 4 CYBER SECURITY INDUSTRY AND PROFESSIONAL DEVELOPMENT

Looking to the Road Ahead	35
State of the Nation	35
What Role Can You Play?	37
Education and Research	37
Business and Industry	37
You, The Individual	38

CHAPTER 5 SECURING OUR CYBERSPACE

Introduction – An Alarming State of Affairs	41
The Paperless World - Digital Transformation During COVID-19	42
Related Cybersecurity	
The Tip of the Iceberg	45
The Rise of Advanced Persistent Threat during Pandemic – APT	45
Group is Increased	
The Attacks on Healthcare Industry during Pandemic	49
The Effectiveness of Threat Intelligence in Predictive Cyber Threats	51
Generic Threat Intelligence Lifecycle	52
Rush Copley Medical Centre Case Study: Success Story of Threats	53
Intelligence Approach Managing Cybersecurity Issues	

Recommended Solution from Expert and Professional in Cybersecurity, or Any Solution Related to Technology How to Manage Impact of Cybersecurity	53
National Active Agencies and Initiative Towards Cybersecurity Issues	54
Malaysia National Security Council	55
National Cybersecurity Agency (NACSA)	56
The Ministry of Communications and Multimedia (KKMM)	56
Cyber Security Malaysia	56
Malaysia Digital Economy Corporation (MDEC)	57
Standard and Industrial Research Institute of Malaysia (SIRIM) Berhad	58
SIRIM QAS	58
MyCERT	59
Human Factor Perspectives: How This Factor Contribute Solve Problem?	60
Empower Cybersecurity Talent through Training and Knowledge Transfer Program	62
Harnessing Technology	65
Security Tactics for People, Processes, and Technology	65
Challenges Deploying and Implementing Security Tactics	67
The Challenges to Make Malaysia Safer	67
Cybersecurity is Everyone’s Responsibility	68
Government, Enforcement Agencies, and Industry Regulator Responsibilities	69
Cybersecurity Professional, Practitioner, Experts and Technology Provider Responsibilities	69
ICT Infrastructure Developer and Business Leader Responsibilities	70
Netizen and Cyber Community	70
 CHAPTER 6 EMERGING FUTURE CYBER THREATS AND TRENDS	
Digital Interconnected World	71
Rapid Growth of Artificial Intelligence Technology	72

Advanced and Sophisticated Phishing Attacks	74
Cyber Terrorism Versus Cyber Warfare	74
Organized Cyber Terrorism	75
Strategic Cyber Warfare	77
The History of Cyber Warfare	77
Are We Ready to Deal with These Challenges?	78
Glossary	81
Bibliography	83
Index	89
Authors' Biographies	91

LIST FIGURES

Figure 1.1	The Threat Vectors by Industry	2
Figure 1.2	The 10 Targeted Industries	3
Figure 1.3	Easy Hacks and Breaches	4
Figure 1.4	The Percentages of the Simple Mistakes and the Cost of Losses	4
Figure 1.5	Top 10 Countries for DDOS Attack	6
Figure 2.1	IoT- A Future of Connected Devices	11
Figure 2.2	The Growth in User-Centric Mobile and IoT Device Will See Greater Exploitation of Personal Data	13
Figure 2.3	The Attack Surface of a Modern Car	16
Figure 2.4	Birth and Rebirth of a Data Breach	17
Figure 2.5	The Wearables	18
Figure 2.6	A Sample of IoT Sensor Types in an Apartment Block Smart City	22
Figure 2.7	The Growing of Cyberattack Surface	22
Figure 3.1	Estimated Global Cybersecurity Spending to 2023	28
Figure 5.1	Device Usage in Malaysia	43
Figure 5.2	The Cause of Ransomware Attack	46
Figure 5.3	Cybersecurity Cases	47
Figure 5.4	Generic Threat Intelligence Lifecycle	52
Figure 5.5	Malaysia Ranking in Global Cybersecurity Initiatives	55
Figure 5.6	Human Factors-Attacker Maliciousness	62
Figure 5.7	The Cybersecurity Workforce Gap by Region	63
Figure 5.8	People, Process and Technology	66

LIST ABBREVIATIONS

IOT	Internet of Things
DDoS	Distributed Denial of Service
ATM	Automated Teller Machine
FBI	Federal Bureau of Investigation
CCTV	Closed-Circuit Television
DVR	Digital Video Recorders
IP	Internet Protocol
GPS	Global Positioning System

PREFACE

Cybersecurity: Everyone Should Alert! provide a basic understanding of the technical aspect of human issues related to cybersecurity in today's digital society. This book outcome from the Research Articulation Grant Scheme (RAGS) by Ministry of Higher Education Malaysia entitled "Exploring the Digital Social Media Cyber Security Risk Factors".

The outcome of the research has a significant impact toward on securing our national cyberspace ecosystem and netizen across the globe due to rapid changes in technology. While technology continues to evolve, the possibilities and threats it presents do so too. We are at a crossroads while we step into the "new age of automation, big data, and the Internet of Things (IoT)" from a world already interconnected with the Internet. But as a civilization primarily based on technology, we are also relying on it as a result. Technology not only brings about even greater benefits but also poses even greater threats: It becomes a focal point for cybercrime, corporate surveillance and cyber-attacks owing to the very existence of the possibilities it provides. Protecting this is, therefore of utmost importance.

This guide examines some of the problems we will soon encounter, including attack vectors like "botnets, autonomous cars, and ransomware, threats like data manipulation, hacking detection, cyber warfare, and ancillary issues like data ownership, digital footprints, the use of innovation in technology". It also gives some insight into the essence of emerging environments and the underpinnings of cybersecurity. On the plus side, as one of the world's fastest-growing markets, Developing our own technology sector allows for economic growth, job creation, and education, ensuring Malaysia remains a technologically advanced nation in the future. Finally, we look at some of the obstacles currently confronted by countries worldwide with respect to cybersecurity, including the need

for stronger cooperation to reduce the threats, education, responsiveness and the balance between privacy and security. Cooperation to reduce the threats, education, responsiveness and the balance between privacy and security.

Our goal is to provide an insightful guide to the relevant cybersecurity issues that Malaysia is facing, to stimulate discussion and debate, and raise awareness of a critical building block of the technologically based community has already been established. As readers will discover throughout this book, cybersecurity is not voluntary. It must be incorporated into the design of each object, database, and electronic communication. Also, we can all protect our future through knowledge, understanding, and positive reform.

Nik Zulkarnaen Khidzir
Wan Nurulasiah Wan Mustapa
Razwan Mokhtar

BOOK OVERVIEW

Cybersecurity: Everyone Should Alert!

The book *Cybersecurity: Everyone Should Alert!* has five chapters consisting of an introduction related to cybersecurity, cyber threats in the information age, cyberspace and digital technology, the future trend of cyber security and securing our cyberspace. Each chapter has a subtopic related to the title of the chapter related to world cybersecurity.

The book begins with the basic concept of cybersecurity. This chapter has a subtopic that tells what happens when cyber security fails to be controlled by humans or users. It also displays ten industry targets and threat vectors for the industry in a data breach, the concept of cybersecurity, and the weakest link for cybersecurity. In addition, this Chapter 1 talks about the world without cybersecurity.

While in Chapter 2, the reader will understand cyber threats in the information age. The beginning of this chapter talks about the human question of why technology is not safe at all. Various types and methods of cybercrime will occur today, with three types of cybercrime that can occur, namely through humans, processes, and technology.

In Chapter 3, the authors focus on the world that depends on technology. It also elaborates on computer security; many opportunities with technology and equal risks always tempt new ideas, products, and lifestyles. Besides, the challenge is also a cyber-attack. Factors of challenges in digital technology and cyberspace are told in this chapter.

Chapter 4, Focus on current world trends related to cybersecurity with technology. Today, all positions, including education and industry, have also given a role to cyber security in technology. This chapter also focuses on information about foreign countries. The United Kingdom (UK) committed within five years to cybersecurity and the federal government's cybersecurity strategy.