CYBER SECURITY EVERYONE SHOULD ALERT

CYBER SECURITY EVERYONE SHOULD ALERT

NIK ZULKARNAEN KHIDZIR
WAN NURULASIAH WAN MUSTAPA
RAZWAN MOKHTAR

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 Fatihah 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 FIGURES

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 toevolve, 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 alreadyinterconnected 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, digitalfootprints, the use of innovation in technology" . It also gives some insight into the essence ofemerging 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 aboutthe 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.