INFORMATION SECURITY AND CYBER LAWS

Prof. Dr. Zoran Gacovski, Ph.D.

a
ArclerPress

Information Security and Cyber Laws

Editor:

Prof. Dr. Zoran Gacovski, Ph.D.

a
ArclerPress
www.arclerpress.com

Information Security and Cyber Laws
Editor: Prof. Dr. Zoran Gacovski, Ph.D.

© 2017 Arcler Press LLC
708 3rd Avenue, 6th Floor
New York
NY 10017
United States of America
www.arclerpress.com

ISBN: 978-1-68094-456-3

Library of Congress Control Number: 2016951154

This book contains information obtained from highly regarded resources. Reprinted material sources are indicated. Copyright for individual articles remains with the authors as indicated. A Wide variety of references are listed. Reasonable efforts have been made to publish reliable data and views articulated in the chapters are those of the individual contributors, and not necessarily those of the editors or publishers. Editors or publishers are not responsible for the accuracy of the information in the published chapters or consequences of their use. The publisher believes no responsibility for any damage or grievance to the persons or property arising out of the use of any materials, instructions, methods or thoughts in the book. The editors and the publisher have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission has not been obtained. If any copyright holder has not been acknowledged, please write to us so we may rectify.

Notice: Registered trademark of products or corporate names are used only for explanation and identification without intent of infringement.

Arcler Press LLC publishes wide variety of books and eBooks. For more information about Arcler Press and its products, visit our website at www.arclerpress.com

INFORMATION SECURITY AND CYBER LAWS

About the Editor

Prof. Dr. Zoran Gacovski, Ph.D.

A native of Rhode Island, in the U.S., Alexandra obtained her Bachelor's degree in History from Johns Hopkins University and her Master's in Media and Communications from the London School of Economics. Her Master's dissertation examined blogs through the lens of psychoanalysis. Alexandra has worked internationally in Prague, Marseille, Tel Aviv, New York and Seattle in various communications and marketing positions in industries such as consumer goods, technology and event production. Her current interests lie in editing and corporate content development.

List of Contributors

K. K. Sindhu
Computer Engineering Department, Shah and Anchor Kutchhi Engineering College, Mumbai, India

B. B. Meshram
Computer Engineering Department, Veermata Jijabai Technological Institute, Mumbai, India

Fredrik Johansson
Swedish Defence Research Agency (FOI), Stockholm, Sweden

Lisa Kaati
Swedish Defence Research Agency (FOI), Stockholm, Sweden
Uppsala University, Uppsala, Sweden.

Amendra Shrestha
Uppsala University, Uppsala, Sweden.

Jiexun Li
College of Business, Oregon State University

Alan G. Wang
Pamplin College of Business, Virginia Tec

Bogdan Denny Czejdo
Department of Mathematics and Computer Science, Fayetteville State University, Fayetteville, USA

Erik M. Ferragut
CSIIR Group, CSE Division, Oak Ridge National Laboratory, Oak Ridge, USA

John R. Goodall
CSIIR Group, CSE Division, Oak Ridge National Laboratory, Oak Ridge, USA

Jason Laska
CSIIR Group, CSE Division, Oak Ridge National Laboratory, Oak Ridge, USA

Huansheng Ning
School of Electronic and Information Engineering, Beihang University, Beijing, China

Hong Liu
School of Electronic and Information Engineering, Beihang University, Beijing, China

Shuai Yuan
SUNY at Buffalo, Buffalo, NY 14260, USA

Raghav H Rao
SUNY at Buffalo, Buffalo, NY 14260, USA

Shambhu Upadhyaya
SUNY at Buffalo, Buffalo, NY 14260, USA

Hongxu Yin
The Power Company of Dezhou, Shandong, Dezhou, China
Rui Xiao
College of Mechanical & Electrical Engineering, Jiaxing University, Jiaxing, China

Fenfei Lv
The Power Company of Dezhou, Shandong, Dezhou, China

Shengxuan Wei
School of Electric Power, South China University of Technology, Guangzhou, China

Qianjin Liu
School of Electric Power, South China University of Technology, Guangzhou, China

Goutham K. Chalamasetty
Department of Electrical and Computer Engineering, The University of Texas at El Paso, El Paso, TX, USA

Paras Mandal[1]
Department of Electrical and Computer Engineering, The University of Texas at El Paso, El Paso, TX, USA

Tzu-Liang (Bill) Tseng[2]
Department of Industrial, Manufacturing, and Systems Engineering, The University of Texas at El Paso, El Paso, TX, USA

Bruce Wardhaugh
University of Manchester School of Law

Claire Bessant
Principal Lecturer, Northumbria Law School

Samson Yoseph Esayas
Norwegian Research Center for Computers and Law (NRCCL), Department of Private Law, University of Oslo

Yohannes Eneyew Ayalew
School of Law, Samara University, Samara, Ethiopia

Rabiah Ahmad
Center for Advanced Computing Technology, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM), Melaka, Malaysia

Zahri Yunos
Center for Advanced Computing Technology, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM), Melaka, Malaysia

Shahrin Sahib
Center for Advanced Computing Technology, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM), Melaka, Malaysia

Mariana Yusoff
Centre for Languages and Human Development, Universiti Teknikal Malaysia Melaka (UTeM), Melaka, Malaysia

Rabiah Ahmad
Center for Advanced Computing Technology, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM), Melaka, Malaysia

Zahri Yunos
Center for Advanced Computing Technology, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM), Melaka, Malaysia

Jacob R Scanlon*
Predictive Technology Laboratory, Department of Systems and Information Engineering, University of Virginia, Charlottesville VA, USA

Matthew S Gerber
Predictive Technology Laboratory, Department of Systems and Information Engineering, University of Virginia, Charlottesville VA, USA

Lorraine Bowman-Grieve
School of PsychologyUniversity of Lincoln

Robyn Torok
Security Research Institute, Edith Cowan University, Perth, Australia

Preface

In today's inter-connected world, the security and the privacy of digital data are primary concerns for all governments and businesses. Virtually no one is protected from the cybercrime on the internet. The term cybercrime originates since the year 2000 when the book with the same name was first published (edited by Thomas and Loader). Cybercrime is defined as computer-initiated illegal activity realized over the global electronic network. Many national governments have adopted their own legislations in the areas of cybercrime and information security. These laws cover different sectors of the economy and the society, such as banking and e-commerce, telecommunications, health, transport (air, sea, rail and road), power and water supply, and education. The adopted laws and standards define different information security measures. Some of these involve security checks, physical security, data safety, security of information systems, and industrial security measures. Importantly, the adopted national information security and cyber laws make sure that all attackers (intruders) who initiate and/or realize attacks are sued and accordingly punished. There are also regional cyber laws, such as European Union's Network and Information Security Directive (NISD), which extend national borders and apply to all the associated member states. This edition covers different topics from cyber security and anti-cybercrime laws, including cyber-criminal detection and prevention, cyber security in different society segments, cyber laws, and cyber terrorism.

Section 1 focuses on cyber-criminal detection and prevention, describing digital forensics and cybercrime data mining, time prints for identifying social media users, a framework of identity resolution, and network intrusion detection and visualization using aggregations.

Section 2 focuses on cyber security in different society segments, describing cyber-physical-social based security architecture for Internet of Things (IoT), emerging issues for education in electronic health records, analysis of causes and events on electric power infrastructure impacted by cyber attacks, quantitative methodology to assess cyber security risk of smart grid, and SCADA framework incorporating MANET and IDP.

Section 3 focuses on cyber laws, describing regimes and mobile telecoms regulation in the twenty-first century, the directive 95/46/EC and the data protection act 1998, the role of anonymization and pseudo-nymisation under the EU data privacy rules, and cyber warfare under the International Humanitarian law.

Section 4 focuses on cyber terrorism, describing the perception on the cyber terrorism, an application of mixed method in developing a cyber terrorism framework, an automatic detection of cyber-recruitment by violent extremists, a psychological perspective on virtual communities supporting terrorists, and an explanatory model for the process of online radicalization and terrorism.

Editor

Prof. Dr. Zoran Gacovski, Ph.D.

INTRODUCTION

Information security, sometimes shortened to InfoSec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).

IT security

Sometimes referred to as computer security, information technology security is information security applied to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber-attacks that often attempt to breach into critical private information or gain control of the internal systems.

Threats

Computer system threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion. Most people have experienced software attacks of some sort. Viruses, worms, phishing attacks, and Trojan horses are a few common examples of software attacks. The theft of intellectual property has also been an extensive issue for many businesses in the IT field. Intellectual property is the ownership of property usually consisting of some form of protection. Theft of software is probably the most common in IT businesses today. Identity theft is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information. Theft of equipment or information is becoming more prevalent today due to the fact that most devices today are mobile.

Cell phones are prone to theft and have also become far more desirable as the amount of data capacity increases. Sabotage usually consists of the destruction of an organization's website in an attempt to cause loss of confidence to its customers. Information extortion consists of theft of a company's property or information as an attempt to receive a payment in exchange for returning the information or property back to its owner. There are many ways to help protect yourself from some of these attacks but one of the most functional precautions is user carefulness.

Information Security Consultant

An information security consultant is also called a cyber or information technology (IT) security professional. Workers in this job are responsible for safeguarding computer systems. Information security personnel often work for governmental agencies and corporations, as well as non-profit organizations. Common tasks for IT security consultants include securing networks from hackers and preventing viruses from harvesting or damaging computer files.

In the modern world, businesses and organizations often depend on computer networks and the Internet to operate. While these connections can bring many opportunities, they also expose computers to potential threats. Malicious attacks on computer systems are not uncommon, and can occur as both automated viruses and targeted security breaches. Regardless of the source, computer security problems can result in sensitive data such as customer credit card numbers and business records being stolen.

IT security experts are retained by organizations and paid to locate and fix vulnerabilities. Consultants often work as independent freelancers, and advise several different clients simultaneously. An information security consultant does not need to have a formal education, and many are self-taught. A degree in computer science and industry-recognized certification in system security is often helpful, however. Many consultants depend on referrals for business, and the previous track record of a cyber-expert is very important.

The technical duties of an information security consultant can vary widely, depending on the needs of a client. Many cyber professionals provide general security services, such as installing antivirus programs and network firewalls for customers.

If a client is concerned about a specific type of breach, such as the theft of financial data, security consultants may focus on proactively testing a system for security flaws. Viewing a network through the eyes of a hacker allows consultants to fix security holes before a vulnerability is exploited.

While the major focus of an information security consultant is to prevent computer attacks before they occur, cyber experts can also take action after a breach has been discovered. Some IT professionals provide services to stop malicious hacking while it is still in progress. These individuals must work against the clock to isolate and fix a detected security leak quickly. An information security consultant might also be tasked with investigating an event after data theft has occurred. Like other types of investigators, IT experts must methodically collect evidence to find the perpetrator of a cybercrime and provide advice to prevent the offense from reoccurring.

Cyberspace

Cyberspace can be defined as an intricate environment that involves interactions between people, software, and services. It is maintained by the worldwide distribution of information and communication technology devices and networks. With the benefits carried by the technological advancements, the cyberspace today has become a common pool used by citizens, businesses, critical information infrastructure, military and governments in a fashion that makes it hard to induce clear boundaries among these different groups. The cyberspace is anticipated to become even more complex in the upcoming years, with the increase in networks and devices connected to it.

Cyber security

Cyber security denotes the technologies and procedures intended to safeguard computers, networks, and data from unlawful admittance, weaknesses, and attacks transported through the Internet by cyber delinquents. ISO 27001 (ISO27001) is the international Cyber security Standard that delivers a model for creating, applying, functioning, monitoring, reviewing, preserving, and improving an Information Security Management System.

Cyber security Policy

The cyber security policy is a developing mission that caters to the entire field of Information and Communication Technology (ICT) users and providers. It includes –

- Home users
- Small, medium, and large Enterprises
- Government and non-government entities

It serves as an authority framework that defines and guides the activities associated with the security of cyberspace. It allows all sectors and organizations in designing suitable cybersecurity policies to meet their requirements. The policy provides an outline to effectively protect information, information systems and networks.

It gives an understanding into the Government's approach and strategy for security of cyber space in the country. It also sketches some pointers to allow collaborative working across the public and private sectors to safeguard information and information systems. Therefore, the aim of this policy is to create a cybersecurity framework, which leads to detailed actions and programs to increase the security carriage of cyberspace.

Cybercrime

Cybercrimes are generally defined as any type of illegal activity that makes use of the Internet, a private or public network, or an in-house computer system. While many forms of cybercrime revolve around the appropriation of proprietary information for unauthorized use, other examples are focused more on an invasion of privacy. As a growing problem around the world, many countries are beginning to implement laws and other regulatory mechanisms in an attempt to minimize the incidence of cybercrime.

Sometimes referred to as electronic crime, one of the most prolific examples involves utilizing a computer connection and specially developed software in order to steal identities, credit card numbers, or other data that the criminal can use to his or her advantage. Using illegally obtained data, the criminal can open accounts, charge a wide range of goods and services, and then abandon the accounts. This leaves the victim in the position of having to deal with huge debts that he or she did not generate.

Blackmail is a long-established illegal act that has been given a new twist in the modern age. The blackmailer may threaten to release embarrassing or other harmful information via the Internet or a private network if the victim does not comply with the demands of the criminal. A cybercrime of this type may go as far as having the victim transfer funds to an untraceable bank account using some type of online payment program, thus making full use of modern technology to commit the crime.

Cybercrime can also involve illegal access to company information. Just as with individuals, criminals can steal financial information and make purchases using the