

Detailed Table of Contents

Preface..... xvi

Acknowledgment xxi

Section 1 **Identifying Cybersecurity and Its Threats**

This section explores and identifies various issues and concerns specific to cybersecurity and some of the policies that accompany them. This section goes into detail with some chapters focusing on economic factors as well as across international borders.

Chapter 1

An Exploration Regarding Issues in Insider Threat..... 1

Jaeung Lee, Louisiana Tech University, USA

Anu Mary Eapen, Infosys Limited, USA

Md Shamim Akbar, The State University of New York at Buffalo, USA

H. Raghav Rao, The University of Texas at San Antonio, USA

Insider threat occurs when a person with legitimate access misuses his privileges and compromises the operations and security of a company. When an outsider tries to gain access to company data, it can often be managed or detected by having standard controls in place. However, when an insider who has rightful access to the data is involved, it can often go undetected. There has been a steady rise in the number of cases of insiders' threat related incidents in recent years. An insider could do this either for his own benefit or might be acting as an espionage to profit another individual or organization. Insider threat is prevalent in various forms across various disciplines and is a serious cause of concern for the operation of an organization and maintenance of trust of the customers. In this chapter, we will look at various forms of insider threats, some well-known insider threat cases, factors causing this kind of behavior, some of the key indicators and what organizations can do to deter the theft of intellectual property.

Chapter 2

The Development of Cybersecurity Policy and Legislative Landscape in Latin America and Caribbean States 24

Indianna D. Minto-Coy, University of the West Indies, Jamaica

M. Georgia Gibson Henlin, Henlin Gibson Henlin, Attorneys-at-Law, Jamaica

The rise and evolution of telecommunications networks over the last few decades have brought immeasurable benefits. Attention to the negative side of these developments has been slow, particularly in the Small Island Developing States of the Caribbean where countries are slowly becoming aware of the developmental, social and economic challenges posed by cybercrimes. Attention has largely been on developed states. However, the experiences covered here add to the global picture on the state of cyber security, increasing understanding of alternative experiences and where they sit alongside the more popular ones such as the US. The chapter details some major development in cyber security in the Caribbean, examining the development of the legal, institutional and organizational landscape in response to growing internal and external cyber threats. Main players and efforts are identified. Information was gathered from interviews and content analysis and the authors' first-hand knowledge.

Chapter 3

Internet Pharmacy Cybercrime: State Policy Mitigating Risks 2000-2015..... 54

Mary Schmeida, Kent State University, USA

Ramona S. McNeal, University of Northern Iowa, USA

Internet pharmacy social gains are efficiency, improving pharmaceutical access for isolates, and less cost. Alongside gains, illegal Internet pharmacies and unscrupulous pharmacy practices have made online purchasing a cyber risk for consumers. Industry self-regulation has failed, giving way to U.S. government and transnational intervention. The U.S. assumes “responsible domestic governance” in disrupting Internet crime by passing modern day drug policies, and having transnational cooperation. States have joined the federal to pass laws generally on licensed in-state entities processing orders for rogue Internet pharmacies but not uniformly. However, online pharmacy sites continue to dispense without “valid” prescriptions, unapproved drugs are sold online, and illegal pharmacies continue to operate. This chapter explores why some American states have adopted laws regulating Internet pharmacies from 2000 through 2015, using Cox proportional hazards regression.

Chapter 4

Identifying and Analyzing the Latent Cyber Threats in Developing Economies..... 74

Atul Bamrara, Indira Gandhi National Open University, India

Internet usage has increased significantly across developing economies in last decade and most of the enterprises are extensively reliable on computer networks for electronic mails to payment gateways. But, the scenario we live in today has become more and more connected, sophisticated and risk-prone to our network-delivered society. Nevertheless, it remains critical for enterprises to exploit the full potential of available technologies such as mobile computing, smart computing and cloud computing. A cyber security related gaffe in any of these rapidly emerging domains may lead to lost productivity and grave concerns to the enterprise. The chapter highlights the various concerns associated to cyber security, viz., how an attack may be operated and offered measures to secure the network and information technology resources within and outside the enterprise. In most of the developing economies no synchronized activities in this regard are taking place which opens the opportunity to cyber criminals intrude into the system and compromise the resources.

Section 2 Cybercrime

This section discusses various breaches, investigations, and crimes that relate to cyber threats and instances. The focus is primarily on detection and analyzing at both the domestic and international areas.

Chapter 5

Cybercrime Investigation 96

Sujitha S., Thiagarajar College of Engineering, India

Parkavi R., Thiagarajar College of Engineering, India

This book chapter will be an introduction to hacking, DDOS attacks and Malware Analysis. This chapter will also describe about the cyber-crime against properties and Persons and will give a detailed description about the cyber security and privacy. This chapter will deal with the cyber-crime investigations, law enforcement policy and procedures. This chapter will also describe about the peer supporting programs for the law enforcement authorities and a detailed description about the control devices and techniques that are used by an officer. This chapter will give an opportunity to know about the evidence collecting procedures in cyber-crime and also the barriers to cybercrime investigations.

Chapter 6

Cybercrimes via Virtual Currencies in International Business..... 121

Dincer Atli, Uskudar University, Turkey

This chapter is willing to shed some light on virtual currencies (VCs) and cybercrimes in International Business. In recent years, Cybercrime is a major concern for the global community. Besides, virtual currency (VC) has made a transformational impact on purchasing habits on a global scale. The advantages VC provides and the difficulty to control it cause the problem of the possibility of committing cybercrimes in the virtual environment. The freedom of VCs provides and the difficulties in controlling it facilitate the realization of crimes like money laundering and finance of terrorism in the virtual environment. Our research demonstrates the structural and legal status of VCs, the different regulations in various countries and the cybercrimes committed via VCs.

Chapter 7

Cybersecurity and Data Breaches at Schools..... 144

Libi Shen, University of Phoenix, USA

Irene Chen, University of Houston – Downtown, USA

Anchi Su, University of California – Los Angeles, USA

Has anyone considered his/her family information going viral and through his/her trusted, chosen school district? This is an age where a mis-sent e-mail with student data can represent enormous liabilities, and a lost laptop can cause newspaper headlines. School institutes are facing new cyber security challenges in the Information Age. A number of school institutes were grappling with the loss of confidential information and protecting students on the Internet. How should school authorities react in case of data breach? What should they do to prevent data breaches at schools? What are upcoming trends in cybersecurity? The purpose of this chapter is to explore data breaches at K-12 schools as well as to examine the ways to improve cybersecurity. In this chapter, the researchers attempt to provide suggestions, solutions, and recommendations on cybersecurity after examining the problems of data breaches.

Chapter 8

Detection Protocol of Possible Crime Scenes Using Internet of Things (IoT) 175

Bashar Alohal, Liverpool John Moores University, UK

Forensics is a science that deals with using scientific principles in order to aid an investigation of a civil or criminal crime. It is a system of procedures that allow an investigator to use as much resources as possible in order to come up with a conclusion for an investigation. Since forensics is a very general term that encompasses an investigation process using scientific knowledge, one can separate a system of investigation based on how it is conducted. This chapter introduces of

internet of things (IoT) forensics, IoT application in forensics field. Art-of-states for IoT forensics are provided. The issues for IoT forensics are identified. Also, we have introduced the proposed data classification in Iot forensics protocol. At the end of this chapter, we point out a brief summary and conclusion.

Section 3 Into the Cloud

This section focuses on the User-End and deploying cloud bases security services through applications, data centers and other enterprise entities.

Chapter 9

Solutions for Securing End User Data over the Cloud Deployed Applications 198

*Akashdeep Bhardwaj, University of Petroleum and Energy Studies
(UPES), India*

With more and more organizations working on the cloud over unsecure internet, sharing files and emails and saving them on cloud storage imperative. Securing the end user sensitive data in transit has thus started to get maximum priority to protect it from Cloud company staff, hackers and data thieves. In this study, an attempt is made to review the research of end user data security. There is an urgent need for solutions for end users' data protection, privacy and during the times when migrating from one Cloud service provider to other. This chapter identifies end user data challenges and issues on cloud and presents use of Public Key Cryptography, Multi Factor Authentication and use of Cloud Aware applications as possible solutions.

Chapter 10

Cloud Computing and Cybersecurity Issues Facing Local Enterprises..... 219

Emre Erturk, Eastern Institute of Technology, New Zealand

This chapter sets out to explore new trends in cyber and cloud security, and their implications for businesses. First, the terminology and assumptions related to cloud computing are stated. Next, the chapter reports on contemporary research around the awareness of security issues, and the security processes within the cloud computing realm. Cyber security poses a different challenge to local small and medium sized organizations, which may seem to have less at stake financially. However, they are more vulnerable, due to fewer resources dedicated toward prevention. A series of serious security incidents may even keep them out of business. Furthermore, security needs to be understood and handled differently in a cloud based environment. Therefore, the chapter identifies unique security practices and recommendations for these businesses to run their IT resources safely in the cloud.

Chapter 11

SOHO Users' Perceptions of Reliability and Continuity of Cloud-Based Services 248

Cornel L. Levy, Western Governors University, USA

Nilsa I. Elias, Western Governors University, USA

The adaptation of cloud computing services is continually growing because of its popularity, its ubiquitous, ease-of-use, and inexpensive nature. Small office/home office (SOHO) businesses are joining large organizations and purchasing cloud services to help with the continuity of their business services. However, cloud computing and its effect in business continuity and information security by SOHO users is not well understood. A qualitative case study was conducted to examine the perspectives of SOHO users of cloud services during Hurricane Sandy in the states of New York and New Jersey. SOHO cloud users were questioned about their understanding of cloud services for business continuity, the services provided by cloud vendors, and their perceptions about cloud data management and security services. The results of this study demonstrated that SOHO users gravitate to the cloud because of its ubiquitous nature, however, they lack understanding of the business continuity and disaster recovery features and their impact in data security and, their business endurance.

Chapter 12

Big Data Security Framework for Distributed Cloud Data Centers 288

Chandu Thota, Infosys Ltd., India

Gunasekaran Manogaran, VIT University, India

Daphne Lopez, VIT University, India

Vijayakumar V., VIT University Chennai, India

The rapid development of data generation sources such as digital sensors, networks, and smart devices along with their extensive use is leading to create huge database and coins the term Big Data. Cloud Computing enables computing resources such as hardware, storage space and computing tools to be provided as IT services in a pay-as-you-go fashion with high efficiency and effectiveness. Cloud-based technologies with advantages over traditional platforms are rapidly utilized as potential hosts for big data. However, privacy and security is one of major issue in cloud computing due to its availability with very limited user-side control. This chapter proposes security architecture to prevent and secure the data and application being deployed in cloud environment with big data technology. This chapter discuss the security issues for big data in cloud computing and proposes Meta Cloud Data Storage architecture to protect big data in cloud computing environment.

Chapter 13

Robotics: Theory and Applications 311

Kijpokin Kasemsap, Suan Sunandha Rajabhat University, Thailand

This chapter presents the overview of robotics; the types of robotic systems; the overview of swarm robotics; the overview of ambient robotics; core ontology for robotics and automation; robotic industrialization and site automation; robotics, cybersecurity, and online threat protection; the robotic applications in modern health care; the robotic applications in surgery; and the robotic applications in modern education. Recent developments in the robotic age have made robots more intelligent, affordable, and user-friendly in modern operations, ranging from manufacturing to health care. Robotic technologies allow for increased production and profit margin because they can accomplish various complicated tasks faster than humans and can produce sophisticated products with higher quality, less down time, and fewer errors than humans. Many benefits of robotics are recognized in cybersecurity, online threat protection, manufacturing, health care, education, business, and finance in the robotic age.

Compilation of References 346

About the Contributors 398

Index 405