Preface

Due to the increase in internet usage, 9-11, and continued security breaches, cybersecurity has been more and more prevalent over the past 15 years. Cybersecurity issues used to be viewed as something only businesses, government, or private organizations had to be cognizant of however it affects each of us on an individual level as well. Cyberspace is also not as secure as it was several years ago because the increase in technology capabilities, amount of users, and amount of added networks it seems practically impossible to fully secure. Identity theft has become a major concerns with consumers specifically in areas where we have seen breaches from major organizations such as Target, OPM, BlueCross Blueshield, Harvard University, Army National Guard, just to name a few. These breaches have been the subject of some type of cybercrime activity whether they were conducted as an insider threat or a hacking incident from the outside. These incidents bring up serious concerns for us as a nation, individuals, and internationally speaking.

Policy is one of the key aspects that has been in a constant state of writing, rewriting, reviewing, and publishing. The Director of National Intelligence (DNI) stated in the DoD Cyber Strategy 2015, “…the threat of cyber-attack was the #1 threat to the U.S. – ahead of terrorism for the first time since 9/11.” Technology has continued to move faster than we can write policy or determine which laws could be used to prosecute these cyber criminals. For the most part, there are not definitive policies specific for cybercrimes due to the nature of location(s) and defining boundaries. Policy makers and legislation cannot write policy and laws on cyber if they do not know what they are dealing with or the nature of it. Without this type of specific knowledge or at least an understanding, grasping the realm of a cyber incident and how it can occur is much more difficult. Although the members of the United Nations continue to work together to develop policies and procedures for identifying and catching cybercriminals, it is still a very thin line for recovery. When discussing cybersecurity as a whole, it is much more than ensuring firewalls are in place, passwords are protected, and monitors are in place for early detection. The key is overall ensuring that the information is protected
Cybersecurity is not just a defensive strategy but should also have an offensive approach as well to be really secure. Securing your cyber infrastructure needs to have a defense in depth approach where there are layers of security, not just an outer or perimeter level of security. If all there is, is a layer of security on the outside, once the hacker has gained access they are in and the entire system is now vulnerable (Wulf & Jones, 2009). By continuing to increase knowledge and awareness through training, education, and experience from practitioners we help to alleviate being taken by surprise more than just putting up defense mechanisms such as intrusion detections systems, anti-virus software, and other security tools.

THE CHALLENGES

The issues and challenges that we continue to be faced with in the cyber world are specific to policy, law enforcement, response measurements, and education. These are not all of them but for the focus of this book these are the ones that are addressed throughout. The attention of policy makers on cyber security has increased more in the last 5-6 years due to national security issues. Law enforcement lacks forensic training and knowledge necessary to recognize and fight against cybercrimes (Busing, Null, & Forcht, 2005). Although that was very much the situation ten years ago, we haven’t come too much further. Some states and nation states are better off than others due to funding, but for the most part, our law enforcement continues to fall short of this type of education. As mentioned earlier, prosecution is another challenge. Prosecution of cybercrimes are difficult due to lack of jurisdiction identification and time it takes to track exactly where the crime occurred – impact usually difficult to determine until too late (Katsh, 1995; Klosek, 1999). Another area of concern or challenge is the policy making and incident reporting from organizations due to reputation or other matters they deem harmful to their company. Agencies/organizations not reporting cybercrime incidents due to negative publicity, reputation, and economic fallback (H.R. 2016). This book also discusses the ethical challenges within some of the chapters. These ethical challenges include privacy, responsibility, misuse, liability, and even fraud, to name a few. Ethical codes for information security professionals have been established to protect personal identifiable information (PII). It is imperative that on an international level there is transparency in order to develop acceptable, clear security policies while following ethical practices.
The book is organized into thirteen chapters. A brief description of each of the chapters follows:

Chapter 1 explains what an insider threat is and can consist of as well as discusses the ethical implications that occur as a result of this type of action. The chapter goes into detail about the relationship an insider threat has with its victim and the factors that possibly harbor this type of behavior.

Chapter 2 this chapter discusses the number of tools, networks, and evolution of technology and how it has increased cyber security threats over the past several years. It talks about the emerging business opportunities as well as the challenges that accompany these security threats. The focus for this chapter goes into further detail discussing the policies and legislation on an international level, specifically within the Latin American states.

Chapter 3 this chapter identifies where state governance and international governance struggle with legislation issues with Internet pharmacies. There is no uniform way of doing things and there are several factors involved to include the differences between online pharmacies and the typical brick and mortar pharmacies. Cybercrime has hit this industry just like it has others and therefore the impact and need for laws and policies specific to this industry are becoming more and more prevalent.

Chapter 4 this chapter explains how developing countries have been a breeding ground for being affected by cybercrime. Although all countries are targets for cybersecurity criminal activity, it seems as though these developing economies have a lower ability to protect themselves.

Chapter 5 goes into detail about what cybercrime is, types of investigations, what is involved and how cybercrimes are categorized depending on the laws and policies used in enforcement. This chapter provides a detailed explanation from A-Z including specific terms and case study examples.

Chapter 6 discusses how virtual currencies have evolved immensely, and quickly establishing themselves as payment systems and/or options. Virtual currencies provide advantages to typical payment methods however make it difficult to control causing more of a disadvantage to being compromised by cybercrime activity.

Chapter 7 explains the consequences of various information breaches within school systems. These range from unintentional information sent (spillage), lost or stolen laptop/hard drives, or not having updated firewalls and passwords and proper encryption methods. This chapter also discusses options of what schools should do to prevent this and suggestions for these problems.

Chapter 8 explains what the Internet of Things (IoT) is and how it can be used to detect cybercrime activities. IoT is a representation of constant growing network of physical objects where all devices can be assigned to an IP address. By using
these objects collectively, this can aid in the detection of cybercrime activity. The chapter explains how this concept could make it much easier for forensics experts to gather information.

Chapter 9 this chapter reviews the challenges in Cloud computing services regarding end user data, analyzing the issues we are faced with, and presenting solutions to overcome these issues.

Chapter 10 explains how cloud security is a subset of cybersecurity and that information technology virtualization is an important technology that powers cloud computing. It discusses the four cloud enterprise access models and the major risks that are inherently involved with access control and privacy.

Chapter 11 this chapter focuses on the small office/home office (SOHO) businesses with relation to cloud computing services. This explains the details and outcomes from a case study performed on SOHO users and their perceptions and lack of understanding of business continuity and disaster recovery features with regards to cloud services and data security.

Chapter 12 goes into detail about what ‘Big Data’ is, definitions, characteristics, challenges, and potential solutions. It explains the correlation between cloud computing, storage, and architecture with Big Data to also include computing models and applications.

Chapter 13 discusses the various types of robotics that are out there today and their many purposes within our society. The chapter goes on to explain the various functions that robotics plays within our daily lives and how it help people with disabilities, add “personnel” to manufacturing organizations, and even military support were humans possibly cannot perform these activities. Their capabilities enable society to be more productive and technologically advance quicker with these robotics.

Michelle C. Moore  
George Mason University; USA

REFERENCES


H.R. 6066, 114th Cong., 2016
