Detailed Table of Contents

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.

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.

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.

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.

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.

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.

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.