Secure It Up Cyber Insurance Due Diligence

Simplify Cybersecurity. Save time with this methodical, fast approach. Based on interviews with 100s of CISOs and personal experience the authors share insights you could only get from the field. You can even listen into some of the conversations held on the books companion website where you will also find time-saving resources to download. This 3x Amazon 'Best-Seller' co-authored by award-winning author David White and best-selling author Mustafa Ahmed is about the practical implementation of professional cybersecurity. With a nod toward ISO 27001, NIST, CISM and CISSP the book is for those focused on taking a smart and rapid approach. The book introduces simple, structured, fast, effective and practical day to day strategies. The focus is to help security professionals deliver in plain English. ESORMA is a system for building out your security operations. Includes strategies on how make the most of the shortage of technical cybersecurity staff. Free accompanying videos, templates, and checklists. You'll know what to do, when, and how across eight business domain areas. Elegant and fast solutions To increase speed, add value and nail wider-ranging enterprise risks. Includes how to consider the rapid migration to cloud. How to do more with less in the face of regulatory compliance, unrelenting evolution and constant governance. How to turn Staff Awareness into an opportunity. Show frontline colleagues how to be your eyes and ears. How to harden traditional infrastructure to minimise new risks and compromising opportunities for fraud and theft. Without investing even more in infrastructure - chances are you can do so much more with what you already have. How to invest in people, processes and change. Enhanced scoping techniques can be used to focus faster on systems, data, architecture and the ever changing future. Increase accuracy and enhance processes for better security. Devastating enterprise breaches continue to be reported. Clearly a streamlined, effective, faster, easier, more comprehensive approach to address cybersecurity and business needs is an imperative. Designed as a quick start, you are advised to buy this book if you are looking for fast-working, easy suggestions designed to save you time and money and set stronger, more comprehensive protection taking into account recent developments. The bottom line is this: There are real-world, everyday cybersecurity problems we all face. This book shares practical strategies ready for you to apply. Ensure your copy is kept close at hand

If you want to learn the basics of computer networking and how to protect yourself from cyber attacks, then keep reading... Two manuscripts in one book: Computer Networking: An All-in-One

Beginner's Guide to Understanding Communications Systems, Network Security, Internet Connections, Cybersecurity and Hacking Cybersecurity: A Simple Beginner's Guide to Cybersecurity, Computer Networks and Protecting Oneself from Hacking in the Form of Phishing, Malware, Ransomware, and Social Engineering This book delivers a variety of computer networking-related topics to be easily understood by beginners. It focuses on enabling you to create a strong foundation of concepts of some of the most popular topics in this area. We have provided the reader with a one-stop highway to learning about the fundamentals of computer networking, Internet connectivity, cybersecurity, and hacking. This book will have the following advantages: A formal yet informative tone, meaning it won't feel like a lecture. Straight-to-the-point presentation of ideas. Focus on key areas to help achieve optimized learning. Networking is a very important field of knowledge to which the average person may be oblivious, but it's something that is everywhere nowadays. In part 2 of this book, you will take a journey into the world of cybercrimes and cybersecurity. The information is designed to help you understand the different forms of hacking and what you can do to prevent being hacked. By the end of this part, you may decide to pursue a career in the domain of information security. In part 2, you will discover the following: The importance of cybersecurity. A brief history of cybercrime, the different types, and its evolution over the years. The various types of cyber-attacks executed over the Internet. 10 Types of Cyber hackers-the masterminds behind attacks. The secrets of phishing attacks and how you can protect yourself against them. The different kinds of malware that exist in the digital world. The fascinating tools to identify and tackle malware. Ransomware and how attackers leverage technology to make money. 9 security testing methods you can learn to do. Social engineering and how to identify a social engineering attack. Network Security, Web Application Security, and Smartphone security. Examples of different types of hacks and past incidents to emphasize the need for cybersecurity. The topics outlined in this book are delivered in a reader-friendly manner and in a language easy to understand, constantly piquing your interest so you will want to explore the topics presented even more. So if you want to learn about computer networking and cyber security in an efficient way, then scroll up and click the "add to cart" button!

Safety and security are crucial to the operations of nuclear power plants, but cyber threats to these facilities are increasing significantly. Instrumentation and control systems, which play a vital role in the prevention of these incidents, have seen major design modifications with the implementation of digital technologies. Advanced computing systems are assisting in the protection and safety of nuclear power plants; however, significant research on these computational methods is deficient. Cyber Security and Safety of Nuclear Power Plant Instrumentation and Control Systems is a pivotal reference source that provides vital research on the digital developments of instrumentation and control systems for assuring the safety and security of nuclear power plants. While highlighting topics such as accident monitoring systems, classification measures, and UAV fleets, this publication explores individual cases of security breaches as well as future methods of practice. This book is ideally designed for engineers, industry specialists, researchers, policymakers, scientists, academicians, practitioners, and students involved in the development and operation of instrumentation and control systems for nuclear power plants, chemical and petrochemical industries, transport, and medical equipment.

Secure It Up!Cyber Insurance Due DiligenceCreatespace Independent Pub

Cyber security involves protecting organisations from cyber risks, the threats to organisations caused by digital technology. These risks can cause direct damage to revenues and profits as well as indirect damage through reduced efficiency, lower employee morale, and reputational damage. Cyber security is often thought to be the domain of specialist IT professionals however, cyber risks are found across and within organisations. Unfortunately, many managers outside IT feel they are ill equipped to deal with cyber risks and the use of jargon makes the subject especially hard to understand. For this reason cyber threats are worse than they really need to be. The reality is that the threat from cyber risks is constantly growing, thus non-technical managers need to understand and manage it. As well as offering practical advice, the author guides readers through the processes that will enable them to manage and mitigate such threats and protect their organisations.

This book constitutes the proceedings of the First International Conference on Science of Cyber Security, SciSec 2018, held in Beijing, China, in August 2018. The 11 full papers and 6 short papers presented in this volume were carefully reviewed and selected from 54 submissions. The papers focus on science of security; cybersecurity dynamics; attacks and defenses; network security; security metrics and measurements; and performance enhancements.

"Drawing upon a wealth of experience from academia, industry, and government service, this book details and dissects current organizational cybersecurity policy issues on a global scale. Using simple language, it includes a thorough description of each issue, lists pros and cons, documents policy alternatives for the sake of clarity with respect to policy alone, and dives into organizational implementation issues. It also equips the reader with descriptions of the impact of specific policy choices, both positive and negative. This book gives students, scholars, and technical decision-makers the necessary knowledge of cybersecurity policy in order to make more informed decisions"--Provided by publisher. Cyber security has become a topic of concern over the past decade as private industry, public administration, commerce, and communication have gained a greater online presence. As many individual and organizational activities continue to evolve in the digital sphere, new vulnerabilities arise. Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications contains a compendium of the latest academic material on new methodologies and applications in the areas of digital security and threats. Including innovative studies on cloud security, online threat protection, and cryptography, this multi-volume book is an ideal source for IT specialists, administrators, researchers, and students interested in uncovering new ways to thwart cyber breaches and protect sensitive digital information. This book serves as a security practitioner's guide to today's most crucial issues in cyber security and IT infrastructure. It offers in-depth coverage of theory, technology, and practice as they relate to established technologies as well as recent advancements. It explores practical solutions to a wide range of cyber-physical and IT infrastructure protection issues. Composed of 11 chapters contributed by leading experts in their fields, this highly useful book covers disaster recovery, biometrics, homeland security, cyber warfare, cyber security, national infrastructure security, access controls, vulnerability assessments and audits, cryptography, and operational and organizational security, as well as an extensive glossary of security terms and acronyms. Written with instructors and students in mind, this book includes methods of analysis and problem-solving techniques through hands-on exercises and worked examples as well as questions and answers and the ability to implement practical solutions through real-life case studies. For example, the new format includes the following pedagogical elements: . Checklists throughout each chapter to gauge understanding . Chapter Review Questions/Exercises and Case Studies . Ancillaries: Solutions Manual; slide package; figure files This format will be attractive to universities and career schools as well as federal and state agencies, corporate security training programs, ASIS certification, etc. Chapters by leaders in the field on theory and practice of cyber security and IT infrastructure protection, allowing the reader to develop a new level of technical expertise Comprehensive and up-to-date coverage of cyber security issues allows the reader to remain current and fully informed from multiple viewpoints Presents methods of analysis and problem-solving techniques, enhancing the reader's grasp of the material and ability to implement practical solutions

The Oxford Handbook of Cyber Security presents forty-eight chapters examining the technological, economic, commercial, and strategic aspects of cyber security, including studies at the international, regional, amd national level.

Add cybersecurity to your value proposition and protect your company from cyberattacks Cybersecurity is now a requirement for every company in the world regardless of size or industry. Start-Up Secure: Baking Cybersecurity into Your Company from Founding to Exit covers everything a founder, entrepreneur and venture capitalist should know when building a secure company in today’s world. It takes you step-by-step through the cybersecurity moves you need to make at every stage, from landing your first round of funding through to a successful exit. The book describes how to include security and privacy from the start and build a cyber resilient company. You'll learn the basic cybersecurity concepts every founder needs to know, and you'll see how baking in security drives the value proposition for your startup’s target market. This book will also show you how to scale cybersecurity within your organization, even if you aren’t an expert! Cybersecurity as a whole can be overwhelming for startup founders. Start-Up Secure breaks down the essentials so you can determine what is right for your start-up and your customers. You’ll learn techniques, tools, and strategies that will ensure data security for yourself, your customers, your funders, and your employees. Pick and choose the suggestions that make the most sense for your situation—based on the solid information in this book. Get primed on the basic cybersecurity concepts every founder needs to know Learn how to use cybersecurity know-how to add to your value proposition

Ensure that your company stays secure through all its phases, and scale cybersecurity wisely as your business grows Make a clean and successful exit with the peace of mind that comes with knowing your company's data is fully secure Start-Up Secure is the go-to source on cybersecurity for start-up entrepreneurs, leaders, and individual contributors who need to select the right frameworks and standards at every phase of the entrepreneurial journey.

Cyberspace is a ubiquitous realm interconnecting every aspect of modern society, enabled by broadband networks and wireless signals around us, existing within local area networks in our schools, hospitals and businesses, and within the massive grids that power most countries. Securing cyberspace to ensure the continuation of growing economies and to protect a nation’s way of life is a major concern for governments around the globe. This book contains papers presented at the NATO Advanced Research Workshop (ARW) entitled Best Practices and Innovative Approaches to Develop Cyber Security and Resiliency Policy Framework, held in Ohrid, the Former Yugoslav Republic of Macedonia (FYROM), in June 2013. The workshop aimed to develop a governing policy framework for nation states to enhance the cyber security of critical infrastructure. The 12 papers included herein cover a wide range of topics from web security and end-user training, to effective implementation of national cyber security policies and defensive countermeasures. The book will be of interest to cyber security professionals, practitioners, policy-makers, and to all those for whom cyber security is a critical and an important aspect of their work.

This book constitutes the refereed proceedings of the Second International Conference on Decision and Game Theory for Security, GameSec 2011, held in College Park, Maryland, USA, in November 2011. The 16 revised full papers and 2 plenary keynotes presented were carefully reviewed and selected from numerous submissions. The papers are organized in topical sections on attacks, adversaries, and game theory, wireless adhoc and sensor networks, network games, security insurance, security and trust in social networks and security investments.

Master the art of detecting and averting advanced network security attacks and techniques About This Book Deep dive into the advanced network security attacks and techniques by leveraging tools such as Kali Linux 2, MetaSploit, Nmap, and Wireshark Become an expert in cracking WiFi passwords, penetrating anti-virus networks, sniffing the network, and USB hacks This step-by-step guide shows you how to confidently and quickly detect vulnerabilities for your network before the hacker does Who This Book Is For This book is for network security professionals, cyber security professionals, and Pentesters who are well versed with fundamentals of network security and now want to master it. So whether you're a cyber security professional, hobbyist, business manager, or student aspiring to becoming an ethical hacker or just want to learn more about the cyber security aspect of the IT industry, then this book is definitely for you. What You Will Learn Use SET to clone webpages including the login page Understand the concept of Wi-Fi cracking and use PCAP file to obtain passwords Attack using a USB as payload injector Familiarize yourself with the process of trojan attacks Use Shodan to identify honeypots, rogue access points, vulnerable webcams, and other exploits found in the database Explore various tools for wireless penetration testing and auditing Create an evil twin to intercept network traffic Identify human patterns in networks attacks In Detail Computer networks are increasing at an exponential rate and the most challenging factor organisations are currently facing is network security. Breaching a network is not considered an ingenious effort anymore, so it is very important to gain expertise in securing your network. The book begins by showing you how to identify malicious network behaviour and improve your wireless security. We will teach you what network sniffing is, the various tools associated with it, and how to scan for vulnerable wireless networks. Then we'll show you how attackers hide the payloads and bypass the victim's antivirus. Furthermore, we'll teach you how to spoof IP / MAC address and perform an SQL injection attack and prevent it on your website. We will create an evil twin and demonstrate how to intercept network traffic. Later, you will get familiar with Shodan and Intrusion Detection and will explore the features and tools associated with it. Toward the end, we cover tools such as Yardstick, Ubertooth, Wifi Pineapple, and Alfa used for wireless penetration testing and auditing. This book will show the tools and platform to ethically hack your own network whether it is for your business or for your personal home Wi-Fi. Style and approach This mastering-level guide is for all the security professionals who are eagerly waiting to master network security skills and protecting their organization with ease. It contains practical scenarios on various network security attacks and will teach you how to avert these attacks.

Alberto Partida's first book, "itsecuriteers," published in 2010, revealed HOW to create an Information Security team that enables business objectives. "Secure IT Up!," his second book, provides qualitative and quantitative insights that justify WHY the adoption of Information Security measures brings benefits to organisations and facilitates cyber-insurance due diligence processes. In the world we live in, risk management and information risk management are complex fields under continuous development. If you need to justify why applying security to your organisation will provide value to your customers or you are involved in cyber insurance due diligence engagements, "Secure it up!" helps you with a statistically sound quantitative study and a set of reputable literature references. "The recommendations in this book are simple but effective: managers will find them of practical relevance and easy to communicate. They are based on sound empirical research which makes them go beyond consultancy speak." Jean-Noel Ezingeard, Dean and Professor of Processes and Systems Management at Kingston University, London. "Alberto Partida combines a comprehensive analysis of existing literature and the results of surveys of subject matter experts to make his argument for combining Enterprise Risk Management (ERM) with information security practices." Richard Stiennon, Chief Research Analyst at IT-Harvest, Author of "Surviving Cyberwar,""Cyber Defense: Countering Targeted Attacks," Blogger at forbes.com, Michigan. Alberto is an information security analyst. He blogs at securityandrisk.blogspot.com and tweets as @itsecuriteer.

When it comes to cybersecurity, everyone needs to be part of the solution if we ever hope to slow the rising tide of cyberattacks Nearly 4.5 billion people—about 60% of the world’s population—were actively online last year. Every one of these individuals conducted business, shopped, handled their finances or browsed for information using a computer, tablet, smartphone or some other connected device at home or work. But while greater global connectivity brings a wealth of benefits, we often fail to recognize that all of these connected people pose a potential cyberthreat to themselves and those around them. As consumers, we have reached an important crossroads; we want high-tech companies and government agencies to protect us from cyberthreats, yet we, too, bear responsibility for securing our connected systems and data. If we ever hope to slow the rising tide of cyberattacks, everyone needs to be part of the solution.

Imagine Yourself... Having control over the websites your kids are visiting and the chat programs they use.. Never worry about getting your computer hacked, your credit card information stolen, family photos taken from you and your everyday life put at risk.. Having the best online safety systems sat up immediately to protect your business from hackers.. If so, you''ve come to the right place. Most, if not all, of us who use technology are familiar with the concept that we need to protect ourselves online. Cyber security is all about taking meaningful steps to ensure that we do not fall victim to hackers. Many people think that employing adequate cyber security means that they download a free antivirus package every year, which will completely protect them and any data and information on their computers. This antivirus will ensure that no malicious files are never downloaded, that they do not access any websites that could be dangerous, that their identities will never be stolen, and that they are generally perfectly safe online. However, this idea is simply not true. Hackers are growing more pernicious and sophisticated every year. They have access to an entire arsenal of cyber weapons, which are often exchanged on the black market. Some of these weapons are powerful enough to bring down websites run by governments and even break into computer servers run by the United States. The need for adequate cyber security is so great that companies spend hundreds of millions of dollars every year in order to protect themselves. However, for many, they must learn the hard way before they implement the protections that they need: they do so only after becoming the victims of security breaches. Becoming a victim of a cyber hack can be an incredibly costly, frustrating, and time-consuming process. For companies, the cost can be in the hundreds of millions of dollars. If a corporation is hacked, the personal data of millions of customers can be compromised; the company then may have to reimburse those people for any fraudulent activity that may have occurred due to the hack. The cost in terms of the company''s reputation may be so severe that the company never fully recovers. For individuals, a computer hack can lead to identity theft, which can lead to hundreds of thousands of dollars in fraudulent financial activity. For both companies and individuals, hacks can lead to sensitive data and information stored in a computer to become compromised. This book will show you many easy things that you can do in order to protect yourself online. It details many of the online threats that you can face, such as describing what spyware and backdoors are. In addition to describing the threats, it lists different types of software that you can utilize to protect yourself against those threats. As a bonus, it talks about the different kinds of hackers so that you can be aware of what you are up against. It talks about different methods that hackers use to gain access to your computer and what you can do to shield yourself from those methods being successful against you. Many of the cyber security methods discussed in this book are either free or very, very inexpensive. However, they can save you countless dollars and hours. There is no way to 100% guarantee that you will not become the victim of a computer hacker. However, if you take meaningful steps to protect yourself online, such as the ones described in this book, you will make your computer significantly more difficult to hack. Hopefully, any hacker who has tried to target you will see that you are serious about cyber security and will move on to his or her next target. If you want to learn how to best protect yourself online, this book is definitely for you! Using the measures advised in this book will help keep you safe from online threats and hacks. BUY with ONE-Click NOW!

Cybersecurity is undoubtedly one of the fastest-growing fields. However, there is an acute shortage of skilled workforce. The cybersecurity beginners guide aims at teaching security enthusiasts all about organizational digital assets' security, give them an overview of how the field operates, applications of cybersecurity across sectors and industries, and skills and certifications one needs to build and scale up a career in this field.

The General Data Protection Regulation is the latest, and one of the most stringent, regulations regarding Data Protection to be passed into law by the European Union. Fundamentally, it aims to protect the Rights and Freedoms of all the individuals included under its terms; ultimately the privacy and security of all our personal data. This requirement for protection extends globally, to all organisations, public and private, wherever personal data is held, processed, or transmitted concerning any EU citizen. Cyber Security is at the core of data protection and there is a heavy emphasis on the application of encryption and state of the art technology within the articles of the GDPR. This is considered to be a primary method in achieving compliance with the law. Understanding the overall use and scope of Cyber Security principles and tools allows for greater efficiency and more cost effective management of Information systems. GDPR and Cyber Security for Business Information Systems is designed to present specific and practical information on the key areas of compliance to the GDPR relevant to Business Information Systems in a global context. Key areas covered include: ? Principles and Rights within the GDPR ? Information Security ? Data Protection by Design and Default ? Implementation

Procedures ? Encryption methods ? Incident Response and Management ? Data Breaches

This book explores the political process behind the construction of cyber-threats as one of the quintessential security threats of modern times in the US. Myriam Dunn Cavelty posits that cyber-threats are definable by their unsubstantiated nature. Despite this, they have been propelled to the forefront of the political agenda. Using an innovative theoretical approach, this book examines how, under what conditions, by whom, for what reasons, and with what impact cyber-threats have been moved on to the political agenda. In particular, it analyses how governments have used threat frames, specific interpretive schemata about what counts as a threat or risk and how to respond to this threat. By approaching this subject from a security studies angle, this book closes a gap between practical and theoretical academic approaches. It also contributes to the more general debate about changing practices of national security and their implications for the international community.

Mathematical methods and theories with interdisciplinary applications are presented in this book. The eighteen contributions presented in this Work have been written by eminent scientists; a few papers are based on talks which took place at the International Conference at the Hellenic Artillery School in May 2015. Each paper evaluates possible solutions to long-standing problems such as the solvability of the direct electromagnetic scattering problem, geometric approaches to cyber security, ellipsoid targeting with overlap, non-equilibrium solutions of dynamic networks, measuring ballistic dispersion, elliptic regularity theory for the numerical solution of variational problems, approximation theory for polynomials on the real line and the unit circle, complementarity and variational inequalities in electronics, new two-slope parameterized achievement scalarizing functions for nonlinear multiobjective optimization, and strong and weak convexity of closed sets in a Hilbert space. /divGraduate students, scientists, engineers and researchers in pure and applied mathematical sciences, operations research, engineering, and cyber security will find the interdisciplinary scientific perspectives useful to their overall understanding and further research.

This book constitutes the refereed proceedings of the Second International Symposium on Cyber Security, CSS 2015, held in Coeur d'Alene, ID, USA, in April 2015. The 9 revised full papers presented were carefully reviewed and selected from 20 papers. The papers reflect four areas of scholarly work: permissions and trust evaluation, implementation and management; cloud and device security and privacy; social implications of networked and mobile applications; system and process assessments for improved cybersecurity.

Cyber Security - Essential principles to secure your organisation takes you through the fundamentals of cyber security, the principles that underpin it, vulnerabilities and threats, and how to defend against attacks. Organisations large and small experience attacks every day, from simple phishing emails to intricate, detailed operations masterminded by criminal gangs, and for every vulnerability fixed, another pops up, ripe for exploitation. Cyber security doesn't have to cost vast amounts of money or take a short ice age to implement. No matter the size of your organisation, improving cyber security helps protect your data and that of your clients, improving business relations and opening the door to new opportunities. This pocket guide will take you through the essentials of cyber security - the principles that underpin it, vulnerabilities and threats and the attackers who use them, and how to defend against them - so you can confidently develop a cyber security programme. Cyber Security - Essential principles to secure your organisation Covers the key differences between cyber and information security; Explains how cyber security is increasingly mandatory and how this ties into data protection, e.g. the Data Protection Act 2018 and the GDPR (General Data Protection Regulation); Focuses on the nature of the problem, looking at technical, physical and human threats and vulnerabilities; Explores the importance of security by design; Gives guidance on why security should be balanced and centralised; and Introduces the concept of using standards and frameworks to manage cyber security. No matter the size of your organisation, cyber security is no longer optional - it is an essential component of business success and a critical defence against the risks of the information age. The only questions left are to decide when and where your journey will begin. Start that journey now - buy this book today!

This book constitutes the refereed post-conference proceedings of the 19th International Conference on Information Security, ISSA 2020, which was supposed to be held in Pretoria, South Africa, in August 2020, but it was held virtually due to the COVID-19 pandemic. The 10 revised full papers presented were carefully reviewed and selected from 33 submissions. The papers deal with topics such as authentication; access control; digital (cyber) forensics; cyber security; mobile and wireless security; privacy-preserving protocols; authorization; trust frameworks; security requirements; formal security models; malware and its mitigation; intrusion detection systems; social engineering; operating systems security; browser security; denial-of-service attacks; vulnerability management; file system security; firewalls; Web protocol security; digital rights management; and distributed systems security.

The prominence and growing dependency on information communication technologies in nearly every aspect of life has opened the door to threats in cyberspace. Criminal elements inside and outside organizations gain access to information that can cause financial and reputational damage. Criminals also target individuals daily with personal devices like smartphones and home security systems who are often unaware of the dangers and the privacy threats around them. The Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution is a critical scholarly resource that creates awareness of the severity of cyber information threats on personal, business, governmental, and societal levels. The book explores topics such as social engineering in information security, threats to cloud computing, and cybersecurity resilience during the time of the Fourth Industrial Revolution. As a source that builds on available literature and expertise in the field of information technology and security, this publication proves useful for academicians, educationalists, policy makers, government officials, students, researchers, and business leaders and managers.

The internet is established in most households worldwide and used for entertainment purposes, shopping, social networking, business activities, banking, telemedicine, and more. As more individuals and businesses use this essential tool to connect with each other and consumers, more private data is exposed to criminals ready to exploit it for their gain. Thus, it is essential to continue discussions involving policies that regulate and monitor these activities, and anticipate new laws that should be implemented in order to protect users. Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications examines current internet and data protection laws and their impact on user experience and cybercrime, and explores the need for further policies that protect user identities, data, and privacy. It also offers the latest methodologies and applications in the areas of digital security and threats. Highlighting a range of topics such as online privacy and security, hacking, and online threat protection, this multi-volume book is ideally designed for IT specialists, administrators, policymakers, researchers, academicians, and upper-level students.

Cyber threats can evolve with almost unimaginable speed and serious consequences for the nation's security. The Government needs to put in place - as it has not yet done - mechanisms, people, education, skills, thinking and policies which take into account both the opportunities and the vulnerabilities which cyberspace presents. Evidence received by the Committee suggested that in the event of a sustained cyber attack the ability of the Armed Forces to operate effectively could be fatally compromised due to their dependence on information and communication technology. The Committee has asked the Government to set out details of the contingency plans it has in place should such an attack occur. If it has none, it should say so - and urgently create some. The Committee was impressed by aspects of the co-operation and joint working between the MoD and private sector contractors. It welcomed the Government's commitment to foster a vibrant and innovative cyber security sector in the UK including a distinct role for the MoD to deliver military capabilities both to confront high-end threats and to provide a potential offensive capability. The opportunity created by cyber tools and techniques to enhance the military capabilities of our Armed Forces is clear. The MoD needs to explore this thoroughly. For this reason, the Committee supports the use of National Cyber Security Programme funding to develop these capabilities, but also wish to be assured that the MoD will maintain its investment in existing defence intelligence services which provide a vital UK cross-government capability

Introduction to Cyber Security is a handy guide to the world of Cyber Security. It can serve as a reference manual for those working in the Cyber Security domain. The book takes a dip in history to talk about the very first computer virus, and at the same time, discusses in detail about the latest cyber threats. There are around four chapters covering all the Cyber Security technologies used across the globe. The book throws light on the Cyber Security landscape and the methods used by cybercriminals. Starting with the history of the Internet, the book takes the reader through an interesting account of the Internet in India, the birth of computer viruses, and how the Internet evolved over time. The book also provides an insight into the various techniques used by Cyber Security professionals to defend against the common cyberattacks launched by cybercriminals. The readers will also get to know about the latest technologies that can be used by individuals to safeguard themselves from any cyberattacks, such as phishing scams, social engineering, online frauds, etc.

The book will be helpful for those planning to make a career in the Cyber Security domain. It can serve as a guide to prepare for the interviews, exams and campus work.

The role of the government in implementing security measures in cyberspace is examined in this textbook, which was designed for practical use by IT security specialists and managers in both the public and private sectors. Link (U. of North Carolina, Green