Cybersecurity for Decision Makers (2023)

Taylor + Francis (ISBN 9781032334974)

Preface

Kenneth David Strang, USA
Narasimha Rao Vajjhala, Albania

Abstract

This book is aimed at business decision-makers, practitioners in any field, and the academic community. The authors have integrated theory with evidence-based practice to go beyond merely explaining cybersecurity topics. To accomplish that, the editors drew upon the combined cognitive intelligence of 46 scholars from 11 countries, to present the state-of-the-art in cybersecurity. Managers and leaders at all levels around the globe will find the explanations and suggestions useful for understanding cybersecurity risks as well as formulating strategies to mitigate future problems. Employees will find the examples and caveats both interesting as well as practical for everyday activities, at the workplace and in their personal lives. Cybersecurity practitioners in computer science, programming, or espionage will find the literature and statistics fascinating and more than likely a confirmation of their assumptions. Government policymakers will find the book valuable to inform their new agenda of protecting citizens and infrastructure in any country around the world. Academic scholars, professors, instructors, and students will find the theories, models, frameworks, and discussions relevant to support teaching as well as research.

Figure A. Thematic evidence-based keyword topic coverage

The book editors conducted machine learning analytics on the contents to present an evidence-based summary of topic coverage. Figure A is a thematic analysis of the chapter coverage, where the size of the keyword indicates higher frequency and importance within the book. Importance, as an attribute, illustrates that the keywords were significant within the context of the discussion, beyond the frequency count, as revealed using machine learning algorithms.

The results of the thematic analysis were used to organize the book contents, in terms of dividing the chapters into sections, naming the sections, and sequencing the chapters within the sections. In the evidence-based diagram of figure A, it is obvious from the large font size that cybersecurity, organizational decision-making, ethical issues, and ethical measures were the central, most important topics discussed. Many authors touched upon those keywords but in the context of specific industries, applications, and disciplines.

As noted earlier, there were 46 authors from 11 countries spread around the world within most of the continental regions. Figure B is a demographic analysis of the authors. Most authors (29%) were from India, then 21% were from the U.K., 19% were from Australia, 8% from Nigeria, 6% in Malaysia, and another 6% from the USA. The remainder of the authors were evenly spread across South Africa (2%), Argentina (2%), Albania (2%), Brunei (2%), and Sri Lanka (2%).

In terms of book metrics, prior to typesetting, there were 34 submissions, 23 chapters were accepted (at the time of writing), bringing the acceptance rate to 68% (0.6765). Prior to typesetting, there were approximately 250,000 words including references and diagrams.

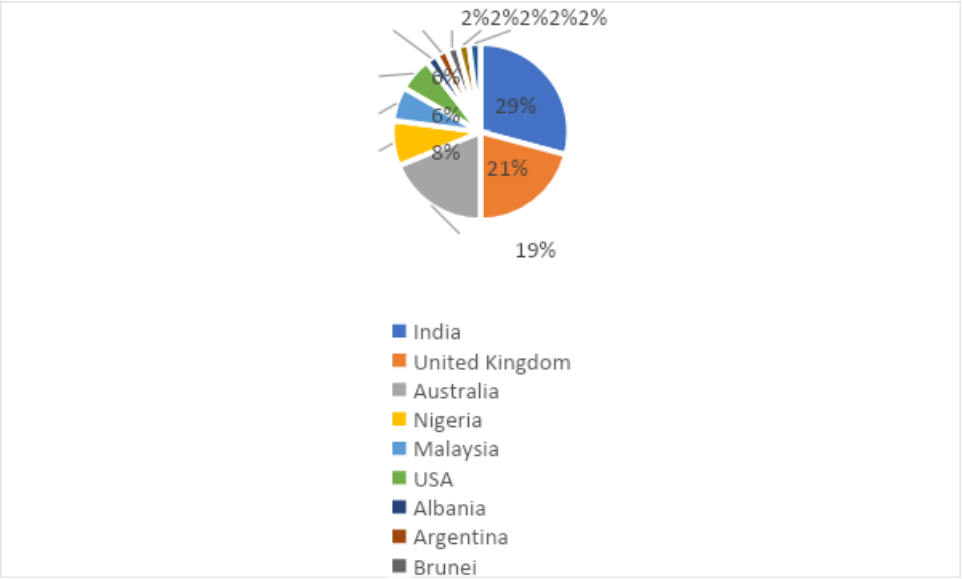


Figure B. Demographics of book authors

Methods and Project Management

The editors applied project management to control the entire book-writing process. The project management was shared between Vajjhala and Strang. As a result, the current book project finished on schedule, it was under budget, within the agreed-upon scope, and the editors assert it has acceptable quality levels. No conflicts of interest were reported by any

team member. Both editors received ethical approval from their respective employers, and no specific external funding was received.

A central website was used to communicate the project's key milestones (http://kennethstrang.com/cyber). Easychair software was used to manage the submission and double-blinded peer review process. Every chapter, including the first one, underwent a double-blind peer review within the Easychair system. At least two reviewers, either an author for another chapter or an external expert, conducted an evaluation using an objective rubric supplied by Strang. Vajjhala served as the managing editor since Strang contributed the first draft of the first chapter as well as developing the evaluation rubric.

Vajjhala conducted most of the administration including the final proofreading, author management in Easychair, and communication with authors. Strang managed the customer relationship management with the other non-author stakeholders. Vajjhala conducted plagiarism checks on all chapters, he investigated any high duplication rates beyond 30% and rejected any chapter with unaccounted-for high duplication rates (to explain, several authors extended earlier papers and declared that in their chapter, so these were accepted at higher duplication rates).

The preface was written as a draft by Strang including the statistical analysis of the keywords and then extended by Vajjhala. As can be seen, by the author demographics, the editors purposely sought to obtain a balanced representation from around the world and especially beyond the traditionally over-weighted North American book-author population. Taylor and Francis Managing Editor, Gabriella Williams (Gabby) and her staff were involved at critical milestones for quality assurance and answering production questions.

Book Content Overview

In Chapter 1 - How Cyber Attacks Disrupt Society and What Decision-Makers Need to Know?, Kenneth David Strang and Narasimha Rao Vajjhala state that government websites and private and public companies have all been hampered by cybersecurity threats. The authors explain that the effects have been severe, affecting daily communications, e-commerce, and the supply chain. This chapter's main research question revolves around that. The authors reveal how cybersecurity attacks have crippled government as well as private and public company sites, around the world. The impacts have been serious including disrupting the supply chain, e-commerce, and everyday communications. Although technology has continued to advance, so have cyber terrorists! In parallel with cyber terrorism, technology has developed exponentially in the last five years, which researchers have expressed as 'Industry 4.0'. Policymakers, academics, and managers working with organizations that use Industry 4.0 technologies and applications should find this chapter interesting.

In Chapter 2 - Onto Nature, Forms and Remedies of Cyberbullying on Social Media Platforms: A Brief Philosophical Perspective, Sooraj K. Maurya posits that technological advancement was one of many good things that came into being with the dawn of modernity. The author explains that despite all the benefits of technology, cyberbullying has emerged as a serious social danger that harms those comfortable using it. As technology has advanced, cyberbullying is now carried out through various platforms, including mobile phones, chat rooms on the internet, blogs, emails, and text messages. The author further explains that

many college students are frequently caught up in some form of digital technology for extended periods. Growing social media use among youth offers cause for severe concern. The author argues that the deliberate, repetitive, and occasionally violent use of communication and information technologies to irritate and harm others is morally unacceptable. The author of this chapter highlights how cyberbullying negatively impacts adults and is a growing global concern. Along with this, the author has tried to identify precise strategies and treatments to deal with the effects of cyberbullying for the betterment of our children.

In Chapter 3 - Cybersecurity and Human Factors: A Literature Review, Natasha Edeh argues that organizations and experts alike have noted that human factors are the "weakest link" in cybersecurity. In most cases, security breaches and incidents that result in significant financial losses in enterprises are caused by intentional and inadvertent human mistakes. The author suggests the use of an interdisciplinary approach to address security challenges has recently undergone a paradigm change. However, there has been little attention paid to and inadequate research done on the topic of human factors and how they might be employed as a cybersecurity solution. The goal of this chapter is to raise awareness of how underutilized human elements in cybersecurity can be used to address problems with cybersecurity. This chapter searched for and examined relevant material on human factors in cybersecurity using a selection procedure. Themes that potentially support the claims that human factors can contribute to organizational security were identified through an analysis of 16 articles.

In Chapter 4 - An Introduction to Cybercrime and Cybersecurity: The Why’s and Who’s of Cybersecurity, Riddhita Parikh explains that cybercriminals may employ various techniques to harm and profit from the victim. The author states that cyber security is the knowledge of numerous procedures that protect the system, networks, and applications against dangerous threats. The author cites recent studies that have found a staggering increase in cybersecurity breaches. The author illustrates examples of cybercrimes linked to banking, credit/debit card fraud, fake social media news, stalking, and bullying. This chapter aims to raise awareness and educate people about cyber security to counteract the threat of e-crime. The history of the digital age, its development, the appearance of cybercrimes and e-securities, and the fact that everyone involved in cyberspace has to know this information to feel secure and safe online are all covered in this chapter.

In Chapter 5 - Cybersecurity Attack Case Studies, Lessons Learned, D.V. Manjula, Aisshwarya Nallamilli, and Dulkarnine Raseeda state that the frequency of cyberattacks is rising gradually as technology advances. The authors argue that these attacks cause significant damage to businesses. The authors give examples of several cybersecurity measures currently used by organizations, including Multi-Factor Authentication (MFA), Virtual Private Networks (VPN), firewalls, and other generic security measures. The authors also illustrate several case studies of cybersecurity attacks that will help decision-makers in organizations. The chapter's goal is to ensure that organizations learn from previous case studies of cyber-attacks and avoid repeating similar attacks. This chapter should help decision-makers to develop policies and prepare for potential cyberattacks.

In Chapter 6 - Towards Cybersecurity Awareness Program for Non-Technical Audience in Malaysia, Shafiq Ul Rehman and Selvakumar Manickam argue that despite all the advantages the Internet offers, people need to be aware that hackers can exploit online

access media to cause significant monetary and material damage to the target audience. The authors state that because cyber-attacks affect enterprises, banking, and the public, cybercrime stands apart from traditional crime due to its diversity, flexibility, dynamism, and ability to evolve. The authors point out that cybercriminals have evolved, becoming more sophisticated and intelligent in their methods of operation due to the intricacy involved in how the economy runs due to the integration of online and Internet technology. This chapter identifies the scams and online fraud cases in the last few years. Based on their findings, the authors created a cybersecurity awareness program to help beginner Internet and technology users avoid becoming victims of cyberattacks and effectively raise long-lasting awareness.

In Chapter 7 - Raising Awareness towards Social Engineering among Adolescents: Psychological and Cybersecurity Perspective, Ruchi Joshi and Shafiq Ul Rehman posit that the ever-evolving technologies ensure the rate of human progress keeps advancing, that we achieve new levels of informational access. The authors focus on social engineering, which is the practice of tricking and manipulating individuals to gain access to vulnerable, sensitive, and intimate data. Social engineering has a psychological, emotional, and occasionally emotional impact on the victim. This chapter aims to shed light on how con artists use psychological strategies to prey on their victims' emotional weaknesses. This chapter also aims to show how social pressure and victims' responses to social cues in conformity, compliance, and obedience causing them to fall for social engineering schemes like phishing, pretexting, baiting, and tailgating. The chapter emphasizes the value of educating students about cyber security and the function of educational institutions, teachers, and counselors in addition to cyber security, legal, and technological specialists. The authors also discuss how social engineering affects people psychologically and the value of mental health experts in offering support.

In Chapter 8 - Intelligent Named Entity-Based Cybercrime Recognition System for Social Media Network Platform, P. Kathiravan, R. Saranya, and P. Shanmugavadivu explore Artificial intelligence (AI) as a technology employed to address the problems of current online threats on social media platforms. The authors focus on the role of natural language processing (NLP) in preventing cybercrime and restricting access to malicious social media posts. The authors illustrate Social Media Post Analysis (SMPA) - a tool for examining interactions between various individuals and groups on social media sites, including Twitter, Facebook, Instagram, and Reddit. SMPA supports the investigation of revolutionary plans and maintains tabs on terrorist actions. The use of a more accurate identification method in Named Entity Recognition is discussed in this study as an essential notion for mitigating cyberattacks on social media networks. Named Entity Recognition (NER) uses various techniques, including rule-based NER, machine learning-based NER, and hybrid NER, to recognize and extract meaningful information from unstructured data, such as Facebook and Twitter comments. With the help of Random Forest and various upgraded RNN architectures like Long Short-Term Memory (LSTM) and BiLSTM, the authors proposed a CyNER system to identify entities like I-Malware, O (others), B-Malware, B-System, I-System, B-Organization, B-Indicator, I-Organization, and I-Vulnerability from a given social media post containing cybersecurity issues. The experimental findings in this chapter demonstrate that the accuracy of the proposed CyNER system is superior to that of BiLSTM and the Random Forest algorithm.

In Chapter 9 - A Case Study on Zonal Analysis of Cyber Crimes over a Decade in India, Diya C. R., Umme Salma M., and Chaitra R Beerannavar argue that despite the immense potential of the Internet, cyberspace is also where most crimes are committed. The authors emphasize that cybercrime is one of the critical aspects of cyber security, which is crucial to information technology and requires urgent attention. This chapter examines cybercrimes in India as a case study. The key source for the analysis is the data gathered from the National Crime Records Bureau (NCRB) from 2010 to 2020. By splitting the geo-locations into seven zones—the central, east, west, north, south, northeast, and union territories—a thorough analysis of cybercrimes across India is conducted in this chapter. The reported cybercrimes in each zone are analysed in this chapter to determine which area necessitates the immediate implementation of security measures. The top 10 states with the highest cybercrime rates are also listed in this chapter. This chapter aims to give a thorough analysis of the crimes and the steps taken to stop them.

In Chapter 10 - Taming the Confluence of Space Systems and Cybersecurity, Syed Shahzad, Keith Joiner, and Felicity Deane emphasize that space systems are essential parts of vital infrastructure, and their removal would have a significant impact on a sizable population, increasingly with safety repercussions. The authors also state that today's digitally connected space infrastructure is vulnerable to sophisticated and destructive cyberattacks in other interconnected cyber systems like banking. The two main categories of these attacks are electronic and cyber. This chapter builds on earlier academic work by making a case for creating engineering, legal, and business frameworks that aim to ensure that space systems are cyber-resilient to present and emerging threats. The research on existing space technologies, attack surfaces, and legal frameworks for their protection and regulation is presented in this chapter.

In Chapter 11 - Regulating Cyber-Physical Systems for Safety Consequences, Mark van Zomeren, Keith Joiner, Lily Qiao, and Elena Sitnikova consider using Cyber-Physical Systems (CPS) within the context of large and complex organizations such as nation-state defense organizations and critical civilian infrastructure. The authors build on a literature review identifying the international best practices for the through-life technical assurance of cyber-capable systems. The chapter expands on the idea of CPS by discussing the social effects of Complex CPS (CCPS). The necessity to examine not only the information assurance components of CPS but also the continual provision of timely and secure physical outputs of CPS is highlighted in the argument for shifting from traditional cybersecurity to cyber-worthiness. This chapter considers the significance of model-based cyber-worthiness evaluations in the framework of monitoring and informing CPS about threats. This chapter explores how emergent aspects of complex CPS may be addressed via cyber-worthiness assessment and Complex Systems Governance (CSG).

In Chapter 12 - Mapping the State-of-the Art: Artificial Intelligence for Decision Making in Financial Crime, Borja Alvarez Martinez, Richard Allmendinger, Hadi Akbarzadeh Khorshidi, Theodore Papamarkou, Andre Feitas, Johanne Trippas, Markos Zachariadis, Nicholas Lord, and Katie Benson provide an overview of recent research on the many uses of AI-based solutions to financial crime problems. The authors employ a multidisciplinary, practitioner-oriented approach that focuses widely on solutions for a financial crime without focusing on a particular criminal typology. This chapter is intended to address potential decision-makers and relevant stakeholders from both industry and

governmental organizations, such as risk or fraud analysts, compliance officers, law enforcement officers, managers in financial institutions, policymakers, and academics with related interests. The aim of the chapter is to enable the decision-makers to assess the capabilities, drawbacks, and specific techniques favoured by researchers when dealing with issues unique to the context of finance. The authors use a chronological approach to describe present methods, new uses, and forthcoming trends, contextualizing artificial intelligence as a useful tool that has not yet been fully utilized.

In Chapter 13 - Understanding and Measuring the Impact of Cyberattacks on Businesses - A Systematic Literature Review, Xiuqin Li, Richard Allmendinger, Elvira Uyarra, and James Mercer examine how cyberattacks impact businesses. The authors identify the gaps in the literature and what future research is needed by systematically evaluating the relevant literature. The COVID-19 epidemic has led to an increase in the number and seriousness of cyberattacks. The authors emphasize that wide-ranging serious corporate damages have resulted from this, including financial losses, reputational damage, decreased productivity, operations disruptions, and complete failure of all business processes. The authors argue that the practice of justifying cybersecurity investment and the future mitigation of cyber hazards would need to be improved by consistent measurement techniques. This chapter's purpose is to contribute to the still-evolving field of cyberattacks from the standpoint of impact measurement. The findings in this chapter provide academics and practitioners with useful information to spot current research trends, influential authors, methodologies, and barriers, identify future research areas, and promote thinking about suitable solutions.

In Chapter 14 - Problems and Ethical issues in Cybersecurity Today: Some Critical Readings, Maximiliano Korstanje examines the problems and ethical issues in the context of cybersecurity from a critical philosophical view. This book chapter critically examines the problems and conundrums surrounding cybersecurity while providing the groundwork for a fresh perspective on the media industry. The chapter advances the argument that global modernity has produced some decentralized modes of production while centralizing essential knowledge, echoing Jacques Ellul and Max Weber's worries.

In Chapter 15 - An Empirical Investigation of Psychological Factors Affecting Compliance with Information Security Organizational Policies, Tatyana Ryutov emphasizes that technological solutions cannot exclusively ensure the security of a company's IT assets. The author posits that information security should also consider human factors. Information security policies (ISP) are frequently violated by employees, which poses a severe risk to businesses. So, the author emphasizes that it is crucial to advance our understanding of voluntary compliance behaviour if we want security measures to work better. By evaluating several user-based risk types, the chapter offers insights on efficiently addressing the issue of ISP non-compliance in enterprises. The author assesses compliance with each of the six main categories of information security policy using decision vignettes, building on a well-supported model of security policy compliance intentions, and comparing model parameters. Practitioners can use the study's findings to strengthen security education and awareness campaigns and improve the protection of organizational assets.

In Chapter 16 - Nexus Between Banking Cyber Security Breaches, Cyber Vulnerabilities and Manifestation of Kidnap for Ransom in Nigeria: A Comparative Analysis

of Kaduna and Abuja Metropolis, Nigeria, Hassan Abdulazeez and Sule Magaji examine the cyberinfrastructure platforms for Nigeria's electronic banking system. The authors state that the simplicity of conducting banking transactions made possible by the system, the decrease in high currency circulation, and the projected consequent impact of lowering crime, such as robberies and corruption, served as the system's central tenets. This chapter looks at how much the system has slowed down, prevented, or even caused the development of additional crimes. This chapter aims to determine the types of crimes that occurred before the cyberbanking security-induced systems regarding the nature and scope of crimes after introducing the system. The chapter uses crime statistical data from the police, conducts interviews with law enforcement officials, and tries to conduct a social survey. The chapter findings reveal a considerable disparity between Kaduna and Abuja in the mean electronic banking and the rise in abduction. The authors recommend that institutions that use electronic banking platforms ensure their hardware and software are constantly functional and frequently submitted to hackproof/integrity checks.

In Chapter 17 - SMEs' Cyber Security Misconceptions: A Guide for Decision-makers, Martin Wilson and Sharon McDonald investigate the attitudes of small- to medium-sized businesses (SMEs) toward adopting cyber security in the UK through a survey of 85 small firms. The findings of this chapter imply that misconceptions regarding the degree of risk to businesses, the nature of cyberattacks, and a general lack of knowledge about cyber security procedures and technologies commonly influence business owners' decisions when interacting with cyber security. The authors consider this information when deciding how to inform SME cyber security decision-makers best and help those who work with SMEs to strengthen cyber security.

In Chapter 18 - Rethinking the Impact of Informal Organizational Rules on Organizational Cyber Security, Maharazu Kasim emphasizes that Information and Communication Technologies (ICT) firms have benefited from technological advancements. However, organizations still need to be concerned about the numerous cybersecurity challenges that have come with it. Organizations must also consider social measures that go beyond even the most robust technological cybersecurity controls. Organizations use formal rules as one of their defenses against both internal and external threats to their systems. Organizations must focus more on the detrimental effects of their internal cyber security. As a result, unofficial regulations are created, which could be harmful to organizational cyber security. This chapter examines the formal and informal rules literature. This chapter aims to understand how formal and informal organizational norms support or undermine organizational cyber security. This chapter's findings showed that although formal regulations can support cyber security, certain situations can undermine it.

In Chapter 19 - Ethical Aspects of Cybersecurity in E-Commerce, Tanya Kumar and Satveer Kaur Data emphasize that cybersecurity is one of the necessities of today's business world because businesses use these systems to safeguard their pertinent data against theft and damage. The authors state that the e-commerce ecosystem suffers financial and reputational harm from cyber-attacks. The authors explain one of the main concerns in e-commerce - privacy protection. The authors posit that implementing cybersecurity ethics in the best way feasible is needed to ensure privacy protection. The chapter lists several ways of demonstrating ethical behaviour, including maintaining confidentiality, privacy concerns, fair policies, avoiding discrimination, respecting intellectual property rights, including copyrights

and patents, and giving back to others and society at large are all examples of ethical behaviour. The chapter aims to identify the ethical concerns surrounding cybersecurity in e-commerce and the ethical controls needed to manage cybersecurity as a pertinent ethical issue in the modern digital world.

In Chapter 20 - Cybersecurity in Healthcare, Arijita Banerjee posits that numerous healthcare companies are targets of cybersecurity threats because of the extensive access to electronic health records. The author explains that due to the rapid development of connected information technology, patients' safety and the reliability of machine learning tools are now at risk, which raises various concerns concerning medical infrastructure. The author explains that in another three years, it is anticipated that cyber events will have caused $10 trillion in global economic losses. Healthcare businesses must therefore highlight the need for flexible cyber defenses. The author emphasizes that hospital breaches have been linked to a lack of cybersecurity understanding. This chapter aims to safeguard information assets and promote a more robust cybersecurity culture across all nations. The author emphasizes that it is crucial to reform new cybersecurity-related legislation and regulations to obtain a comprehensive solution.

In Chapter 21: Business continuity and disaster recovery strategies (BCRS) as resilience tools after cyberattacks in toxic entrepreneurship ecosystems, Lukman Raimi describes how businesses and corporate organizations might respond to unfavourable occurrences and economic turmoil. The author describes business continuity and disaster recovery strategies (BCRS) as resilience measures for dealing with the susceptibility of cyberattacks in unhealthy entrepreneurial environments. The author emphasizes that the use of digital technologies has improved the technical and economic performance of businesses impacting employee productivity, service delivery effectiveness, customer experience and satisfaction, risk management, the detection of human errors, and the precise use of human, financial, and material resources (HFM) in digital workplaces. The author states that the digital age and its associated technologies have seen an increase in cyberattacks that have disrupted businesses, stolen massive amounts of data, caused financial losses, resulted in rapid bankruptcy, and posed risks to entrepreneurship. The chapter aims to discuss eleven (11) different business continuity and disaster recovery strategies (BCRS) that entrepreneurs and corporate organizations can use to thwart cyberattacks in unhealthy entrepreneurial ecosystems. These strategies are based on the plethora of cybersecurity issues and concerns raised in the literature.

In Chapter 22: Building Cybersecurity Capacity through Education, Awareness, and Training, Ruth Shillair, William H. Dutton, Patricia Esteve-Gonzalez, Sadie Creese, and Basie Von Solms offer managers and decision-makers advice on how to prioritize scarce resources as they struggle to safeguard stakeholders against evolving internet dangers. The authors discovered a definite effect of cybersecurity education, awareness raising, and training (CEAT) on the vitality of internet use and services at the national level based on a comparative analysis of 80 countries. The Cybersecurity Capacity Maturity Model for Nations, or CMM, was created by the Global Cybersecurity Capacity Centre and included one of the five components of a wider cybersecurity capacity-building model. The education, awareness, and training indicators that make up this aspect of capacity building within the CMM are briefly discussed in this chapter, along with our cross-national analysis of the results of CEAT on internet use. The quantitative analysis in this chapter demonstrates a

positive and statistically significant impact of CEAT on the vitality of internet use and services while controlling for contextual variables such as country wealth and the extent of internet use. The authors make recommendations for policy and practice to address the need for more successful programs while acknowledging the immaturity of cybersecurity education, awareness raising, and training in most countries reviewed.

In the last chapter of this book - Cybersecurity Awareness: Prerequisite for Strategic Decision-Makers, Sadiq Nasir investigates the principles of cybersecurity awareness (CSA) for people who make strategic decisions for an organization. The authors have undertaken a social-technical approach to present ideas that decision-makers need to be aware of. Additionally, this chapter looks at the cybersecurity-related considerations that must be made by decision-makers. The author emphasizes that a strong CSA from the top will support and safeguard the company's good cybersecurity practices.

Acknowledgments

Associate Professor Narasimha Rao Vajjhala, Albania

I want to thank my family members, particularly my mother, Mrs. Rajeswari Vajjhala, for her blessings and for instilling in me the virtues of perseverance and commitment.

A special note of thanks to co-editor, Professor Kenneth David Strang, for consistently motivating me to continue my research work.

Professor Kenneth David Strang, USA

I'm shouting out a thank you to all our chapter co-authors for cooperating with me to ensure this edited book project was completed on time - their names are published within. Obviously, without our chapter co-author's contributions, Rao and I would have had to do much more work which may have taken more than 20 times as long.

I also think about those people not in the book. I want to extend best wishes and empathy to those emerging scholars who, for one reason or another, were not able to finish their studies in time for publication here. To those colleagues - don't worry there will be other opportunities in the future for you to share your wonderful research.

My co-editor Dr. Narasimha Rao Vajjhala (Rao) has done almost 100% of the administration for this project, including overseeing the laborious peer review processes, and manuscript editing, so he has proven his ability. Rao is on a trajectory to become a global scholar and I am proud to see him grow as a scholar every year.

Mikko Hyppönen helped us by writing the foreword in a short time over the busy Christmas season. I recruited Mikko and selected him due to his industry expertise and his being based in Helsinki, Finland (explained further below). When you read his foreword, I hope you realize he is correct - cyber hacking is pervasive. My best wishes to other practitioners who were evaluated as a possible foreword writer.

Bulcsu Szekely (Bubu) deserves thanks for educating me about contemporary cyber warfare and he influenced me to select a European foreword writer. Bubu works for a university in Finland, and he has lived through cybersecurity warfare. His rich descriptions of what can happen inspired me to include contemporary content. We avoid politics in

scholarship (except if the discipline is political science - which it is not here), but I want to reveal the significance of Bubu's input, as I will summarize below.

Finland shares a very long 830-mile (1,340 km) border with Russia, and I probably don't have to spell out all the details of the Ukraine situation, and Finland's recent emergency application to join NATO. It is clear to me, as an outsider a continent away, based on what I have researched, that many companies, government departments (including medical facilities), and individuals in Finland have experienced financial damage due to cybersecurity warfare.

Past behavior repeats itself - that is a well-known axiom and it has been proven to be true based on psychology discipline research. Russia has a long history of aggressive behavior, including invasions of other countries, often denying their being the aggressor. For example, back in 1939, Russia's Red Army shelled their own Soviet village of Mainila, and blamed Finland by covertly raising a fake flag as an excuse to initiate a war. There have been numerous well-documented Russian invasions, as briefly enumerated below:

- Iran (1941–1946);
- Hungary (1944);
- Romania (1944);
- Bulgaria (1944);
- Czechoslovakia (1944);
- Northern Norway (1944–1946);
- Bornholm, Denmark (1945–1946);
- Germany (1945);
- Austria (1945–1955);
- Manchuria (1945–1946);
- Korea (1945–1948);
- Kuril Islands (1945);
- Czechoslovakia (1968–1989);
- Afghanistan (1979–1989);
- Crimean Peninsula (2014);
- Ukraine (2022+);
  portions adapted from public data at https://www.ghpage.com/tall-list-of-countries-russia-has-invaded-since-1941-drops/221973/).

Russia is considered the second most powerful country in the world (after the USA), from a military perspective. By comparison, the USA has not initiated any such hostile military invasions in over a hundred years. This may be an oversimplification of history, but as an American, I remember from grade school that many years ago the french were killed along the northern border at a time when the USA was attempting to become independent of the British monarchy rule (note that Canada is still formally under the rule of England).

Interestingly, a political confrontation in 1990 made the history books when a small band of Mohawk Indians, who were U.S. citizens, traveled to Quebec at the invitation of the Kanesatake Mohawk Oka reservation, to protest the expansion of a golf course on disputed tribal land. After two months of confrontations, over 100 Quebecois police, backed y 4400 Canadian Army troops, defeated the Mohawks, taking 200 prisoners (including 30 U.S.

citizens). One Quebecois police person was killed and numerous soldiers on both sides were hospitalized for injuries sustained during the fighting (adapted from public data at https://www.mentalfloss.com/article/60380/4-times-us-invaded-canada). The Quebec government subsequently bought the land to stop the development of the golf course and to end the fighting! Back to Bubu, this illustrates my experience pales in comparison to his.

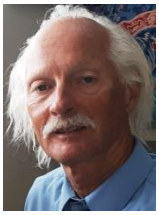
Finally, although I have already mentioned this, I want to thank the staff at Taylor + Francis who accepted our proposal for this book and assisted us to make it a reality.

Editors

Associate Professor Narasimha Rao Vajjhala, Doctorate in Information Systems and Technology
University of New York Tirana, Albania

Dr. Narasimha Rao Vajjhala is working as an Associate Professor and the Chair of the Information Systems department at the American University of Nigeria. He had previously worked at the Faculty of Engineering and Architecture at the University of New York Tirana, Albania. He is a senior member of ACM and IEEE. He is the Editor-in-Chief for the *International Journal of Risk and Contingency Management*, and a former Managing Editor. He is a member of the Risk Management Society, and the Project Management Institute. He has over 20 years of experience in teaching programming, design, security, analytics, and database-related courses at both graduate and undergraduate levels in Europe and Africa. He has also worked as a consultant in technology firms in Europe and has experience participating in EU-funded projects. He has completed a Doctorate in Information Systems and Technology (United States); he holds a Master of Science in Computer Science and Applications (India), and a Master of Business Administration with a specialization in Information Systems (Switzerland).

Professor Kenneth David Strang, Doctorate, MBA, BS, AS, CNA, CSCS, CRP, CPP, FLMI, PMP
W3-Research, USA and RMIT University, Australia



Professor Strang has over 300 publications (http://kennethstrang.com) and at the time of writing he has consistently ranked in the 95-97 percentiles of world-wide scholars at Research Gate. Dr. Strang has been working since 1983. Ken has been employed by W3-Research, a business analytics company, since 2010. He is a retired full professor who occasionally lectures at reputable universities and associations. Ken has a professional Doctorate in project management operations research, an MBA in strategic management, a BS in marketing, and an AS in computer science all with summa cum lade high grade distinctions. He has six professional certification/licenses: Certified Netware Administer (security), a Fellow Life Management Institute (insurance actuary), a Certified Research Professional (scientific research), a Project Management Professional, a Certified Supply Chain Specialist/Procurement Professional, and a World Medical Association research ethics certification. Ken conducts research in business, healthcare, logistics/supply chain, manufacturing, marketing, mining, new product development, leadership, organizational behavior, industrial psychology, tourism marketing, human resource management, learning styles, online learning, nuclear-hydro-solar-wind clean energy production, and procurement project management. He edited a best-selling research design-methods textbook for Palgrave-Springer and he won over $8M USD in grant-proposals to support his clients. He also won two Emerald Literati Awards. He has managed over 115 studies, taught over 1000 multicultural students with an anonymous course opinion survey satisfaction median of 5/5 and a mean of 4.5/5. Ken volunteers for many charities and not-for-profit social advocate associations.