



Navigating New Cyber Risks

How Businesses Can Plan, Build and Manage Safe Spaces in the Digital Age

GANNA POGREBNA
MARK SKILTON

Navigating New Cyber Risks

Ganna Pogrebna · Mark Skilton

Navigating New Cyber Risks

How Businesses Can Plan,
Build and Manage Safe Spaces
in the Digital Age

palgrave
macmillan

Ganna Pogrebna
University of Birmingham
Birmingham, UK
The Alan Turing Institute
London, UK

Mark Skilton
Warwick Business School
University of Warwick
Coventry, UK

ISBN 978-3-030-13526-3 ISBN 978-3-030-13527-0 (eBook)
<https://doi.org/10.1007/978-3-030-13527-0>

Library of Congress Control Number: 2019933311

© The Editor(s) (if applicable) and The Author(s), under exclusive licence to Springer Nature Switzerland AG 2019
This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Cover design by Alexander Kharlamov

This Palgrave Macmillan imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

“If I had a world of my own, everything would be nonsense. Nothing would be what it is, because everything would be what it isn’t. And contrary wise, what is, it wouldn’t be. And what it wouldn’t be, it would. You see?”

Lewis Carroll “Alice in Wonderland”

*For my son Madoc, my husband Alex, and all those wonderful people
who didn't find my quest to beat cybersecurity with a measuring stick
to be positively hysterical*

—Ganna Pogrebna

For my mother Angela

—Mark Skilton

Foreword

Cybercrime is the fastest-growing industry in the world and cybersecurity is the hottest topic on the planet. The one aspect of this topic that has the industry in a quandary is how to identify, protect, contain, and mitigate against cyberattacks on your business, customers, partners, estate, systems, and infrastructure. The variety, complexity, sophistication, and velocity continue to increase and expand at scale; and the threats are endless. While globally organized cybercriminal groups continue to launch increasingly sophisticated attacks against our networks, suppliers, and clients for monetary gain, it appears that some of the oldest and more simplistic techniques have proven to be highly effective and lucrative for these miscreants. For those of us engaged in cyberdefense on a daily basis, social media has become a major enemy, as it is used by cybercriminals to get to unsuspecting citizens as these citizens complain on Twitter, Facebook and other platforms when systems of a particular bank or financial institution are down or not working properly. Adversaries seize the moment to offer assistance, use social engineering to trick innocent victims into giving them private logins and credentials and wipe out their lifetime savings. Due to the scale and velocity with which such malicious activities propagate, the impact of these crimes is devastating. For more than 20 years we have been educating end users about the danger of clicking on a link in an email and, later on, on their smartphone. Yet, phishing attacks based on user-activation of malicious links are still widely used and continue to be extremely effective and profitable. While the largest and most widely known cybersecurity events held each year worldwide fill their floors with suppliers promoting their products and services and claiming to offer “silver bullet” solutions to protect and save

you against cyberthreats; in reality, there is no silver bullet, and the hacks, compromises, and losses continue to increase. Not only financial, but also industrial espionage, counterfeit goods, theft of intellectual property, stealing trade secrets and compromising propriety research and development (just to name a few) continue to grow and threaten the very core of the economic health of our countries and society. Perhaps it is simple: technology alone is not the answer. It is simply a tool; and in the modern digital world the only thing that distinguishes cybercriminal from an honest individual is “opportunity”, or the way in which we take or not take advantage of opportunities which are coming our way. Therefore, cybersecurity is not just a technical science, it is a behavioral science. It is now clear that we keep doing the same thing over and over again (i.e., trying to beat cybersecurity problems with a technological stick), expecting a different result—that is the definition of insanity. Yet, the problems we are facing in cybersecurity not only require a new and different approach, but most certainly a paradigm shift in our thinking. In order to successfully alleviate the risk of cyberattacks, we need to focus on people behind the keyboard or on the other side of the phoneline. We need to understand how they behave, think, act, and react—only by doing this we will be able to predict and, possibly, prevent their criminal actions. The human element of cybersecurity lies at the heart of this book’s analysis, which is based on the real-world examples of how behavioral science can be effective and critical for enhancing our ability to address cybersecurity gaps. Obviously, there does not exist one simple answer to cybersecurity problems. Cybersecurity is constantly evolving, as are the people and minds behind cybercrime. Therefore, we need to be agile and understand that we too must innovate and evolve our thinking, technology, processes, education, and skills, while making full use of the recent breakthroughs in behavioral science.

If you have been working in cybersecurity for decades, or are making your first steps and want to feed your curiosity about this field not only from a risk, compliance, or technology perspective, but also from a behavioral science perspective, then I would say you have already opened your mind to the art of the possible, a new and different approach to the problem. I would then tell you to read on, as this book is the best place for you to start. It will most definitely expand your mind. It challenges the thinking of the most experienced and brightest cybersecurity practitioners as well as offers a nice guideline to cybersecurity as a behavioral science for beginners. It will take you back in time and give you a very thorough overview of where it all started, charting the course of the evolution of cybersecurity and, even more fascinatingly, the evolution of cybercriminal, the criminality, and the

conscience of these nefarious actors. The authors approach this as behavioral scientists, from the viewpoint of someone who was trying to make sense of the field. They adopt the perspective of a typical practitioner (not a technical specialist), someone who is trying to understand the true risks and simply navigate this complex field, by considering alternative cybersecurity solutions and enhancements as well as leveraging the people aspect to improve outcomes and achieve more effective results in building safe digital spaces for business and beyond. The first chapters of the book provide a general summary of the field and systematize the threats. The second part of the book describes how behavioral science (both conceptual and algorithmic) could contribute to solving the majority of cybersecurity issues. Something we can all embrace.

This book offers a different view on cybersecurity and cyberdefense—a behavioral (human) view. Its purpose is to consider how to frame the new threats in the digital and physical world, understand their nature, and formulate cybersecurity responses, which, in the face of the contemporary threats, need to combine both technical and behavioral strategies beyond compliance certification and standards. Security and compliance are not the same; we have to get beyond thinking that being compliant is being secure. The authors call upon recent evidence from leading practitioners and academics and offer new methods which will help organizations to plan, build, and manage cyber risks.

In this book, leading business thinkers and experts came together, combining contemporary visions from cybersecurity, behavioral science, human–data and human–computer interactions, and artificial intelligence (AI) fields, to provide practical insights for businesses and help them anticipate new risks and vulnerabilities, which they have never encountered earlier in digital environments. The authors analyse practical evidence-based cyberthreats and organize expert responses into a practical toolbox on how to consider risks and vulnerabilities across different dimensions, as well as suggesting ways to discover new risks and vulnerabilities. After reading this book, you will gain a better understanding of predictive analysis as well as learn how to anticipate what is coming next (e.g., future threats and vulnerabilities).

This book focuses not only on how new risks and vulnerabilities could be identified but also on human interpretations of these risks and, ultimately, on how the actual threats could be overlooked by humans. It delivers a piece of the puzzle that meets a critical gap in helping to identify ways to embed human behavior into the design of safe human-cyber spaces so these systems operate in the service of making human-centered digital ecosystems more

secure. These ideas help us get closer to security-by-design and must be considered when thinking about the future of security and proactive network defense.

The authors explore whether and to what extent human psychology is prone to different social-engineering tricks, which cybercriminals play on us. Knowing this allows us to use cutting-edge behavioral measures and tools in order to complement the technical solutions which already exist.

This book will help everyone who reads it, no matter how much or how little experience you have in this field. It will give you insights, ideas, and stimulate thoughts, challenging the norm and your usual way of thinking about the problem of cybersecurity. Make no doubt about it: cybersecurity is a systemic and global problem, an arms race complemented by the looming feeling that the criminals are outpacing us in every way. The authors suggest alternative ways to close the existing gap. By treating cybersecurity as a behavioral issue, we can open the door to incredible critical and problem-solving thinking and innovation in this area. Just imagine the exciting possibilities, which behavioral approach can offer! We can algorithmically predict attacks using the behavioral topology of cybercriminals and their business models. This will enable us to design smart active cyberdefense mechanisms by anticipating attacks and collecting forensic evidence “on the fly” when attacks are still in progress. In this book, you will receive practical tips about incorporating behavioral approaches for understanding and improving cybersecurity within your organization and learn how to integrate it into your environment to enhance your holistic approach to building safe digital spaces. There are a number of new ideas regarding the psychology of cybersecurity—behavioral segmentation of users and cybercriminals, new “positive” approaches to cybersecurity campaigns, multilayered cybersecurity systems tailored to different types of cybercriminals, etc.

It is a fascinating read and makes tremendous sense. The authors provide us with well-defined ways of thinking about security and get us one step closer to uncovering the anatomy of the criminal activities and business models and, ultimately, advance us towards finding that silver bullet, which would give us tangible advantages over cybercriminals in the future. Taking human behavior into account when thinking about cybersecurity is extremely important and should not just be a factor we consider after the design of security systems is complete. The reality dictates that we should have a human (and our propensity to make errors, show bias, etc.) in mind when we build secure environments and when we are trying to defend against threats. As I said at the beginning—the problem often boils down to understanding who is behind the keyboard. After all, cybercriminals are

only human: they are just people who exploit those endless opportunities which come their way in the digital age and prey on the innocent without a conscience.

This is a thought-provoking, compelling book that adds a whole new dimension to how we address cybersecurity and cyberdefense from the perspective of human behavior. It is a must-read for cybersecurity practitioners, cybersecurity professionals, researchers, behavioral scientists, and people who are simply interested in this field or worried about their personal security in cyber spaces.

London, UK

Maria Vello
CEO of the Cyber Defence Alliance

Preface

This book brings together leading experts and builds on the latest exciting research advances from cybersecurity, behavioral science, human–data interaction, human–computer interaction, as well as artificial intelligence (AI) fields, in order to offer new practical insights for businesses and help them to identify and address new vulnerabilities in human-cyber spaces. We are particularly focusing on threats and vulnerabilities, which businesses otherwise would not be able to identify in the modern complex digital environments. We consider cyberthreats, most recently and frequently observed in practice, and, organize expert views and opinions into a practical toolkit. This toolkit is intended to help practitioners and business owners to anticipate, consider, and tackle risks and vulnerabilities across different dimensions. It also suggests ways in which new (previously unobserved) risks and vulnerabilities can be discovered by looking at the wider ecosystem of issues beyond data and technology.

Our attention goes beyond traditional detection of risks and vulnerabilities. We pay particular attention to how humans perceive these risks and vulnerabilities and how those perceptions can misrepresent the actual threats, leading to under- or overreaction when responses to threats are formulated. We also look at how the ability to anticipate new risks and vulnerabilities can influence business models and business model innovation. Our goal is to empower businesses to be able to apply a new human-centered vision to cybersecurity problems in order to detect risks which they have not encountered or have not anticipated before. Furthermore, these risks and vulnerabilities do not only have to be detected, but also effectively communicated.

We aim to demonstrate how understanding and effective communication of risk-related issues can help build secure and safe human-cyber spaces in the new digital economy.

This book provides a detailed gap-bridging guide, which explains how to embed human behavior into the design of safe human-cyber spaces. It shows that cybersecurity should not be viewed as a *fixed cost* factor by businesses, which can only be addressed through technological upgrades. It is important to understand, that cybersecurity in many ways depend on humans and there is a need to design and build security systems with humans in mind. While there is a plethora of cybersecurity books, the existing book market offers little guidance on how to anticipate and diagnose new threats related to advanced AI cyberattacks and criminal social engineering, even though these threats are discussed by governments and international forums, requiring the development of new theoretical methodology, empirical tools, as well as policy. What seems to be missing is a way for current business practitioners to understand these new threats and risks and bring these together into an integrated toolkit. The new approach developed in this book helps us to address these issues as it draws upon the ideas and thoughts of leading experts, supported by the practical evidence.

Warwick, UK
January 2019

Ganna Pogrebna
Mark Skilton

Acknowledgements

The development of this book has involved many hours of research and interviews with leading practitioners and academics in the fields of cybersecurity, behavioral science, machine learning, artificial intelligence (AI), economics, and business. We are extremely grateful to **Ms. Maria Vello**, CEO of the Cyber Defence Alliance, who wrote the foreword for this book. Maria's contribution to cybersecurity in the UK and internationally continues to inspire the authors of this book as well as many cybersecurity scholars and practitioners globally. We would like to recognize and sincerely thank the following people who gave their time in discussions, sharing thoughts and ideas that have helped us craft this book: **Debi Ashenden**, Professor of Cyber Security, School of Computing, and Programme Director for Protective Security and Risk at the Centre for Research and Evidence for Security Threats (CREST), University of Portsmouth; **Jon Crowcroft**, Marconi Professor of Communications Systems, Computer Laboratory at the University of Cambridge, Associate Fellow at the Centre for Science and Policy, and Fellow of the Alan Turing Institute; **Anthony Phipps**, cybersecurity expert and Senior Manager leading the Digital Cyber Research team at one of the largest financial institutions in Europe; **Haydn Povey**, CEO and Founder of Secure Thingz and board member of the IoT Security Foundation; **Karen Renaud**, Professor of Cybersecurity at Abertay University, Professor Extraordinarius at the University of South Africa, Fullbright Scholar, Honorary Research Fellow (Computing Science) at the University of Glasgow; **Boris Taratine**, cybersecurity expert, passionate visionary, and an influential ambassador of cybersecurity and cyberdefense; **Tim Watson**, Professor of Cybersecurity and Director of the Cyber Security

Centre at Warwick Manufacturing Group (WMG) at the University of Warwick; **Sir Alan Wilson**, Executive Chair of the Ada Lovelace Institute, Professor of Urban and Regional Systems at University College London, and former CEO of the Alan Turing Institute; **Karen Yeung**, Professorial Fellow in Law, Ethics and Informatics, University of Birmingham, member of the European Union (EU) High Level Expert Group on Artificial Intelligence, and member and rapporteur for the Council of Europe's Expert Committee on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT). We also thank many cybersecurity practitioners from leading financial, legal, and technological industries, as well as experts working in law enforcement, whose work and advice inspired this book but who wished to remain anonymous. Original artwork for this book was produced by **Alexander Kharlamov**, an award-winning artist and photographer, in collaboration with the authors.

Disclaimer

All company names, trade names, trademarks, trade dress designs/logos, copyright images, and products referenced in this book are the property of their respective owners. No company references in this book sponsored this book or the content thereof.

Contents

1	Introduction	1
 Part I New Cyberthreats and Why We Should Worry about Them		
2	Cybersecurity Threats: Past and Present	13
3	A Sneak Peek into the Motivation of a Cybercriminal	31
4	Wake Up: You Are the Target!	55
 Part II Existing Solutions and Cybersecurity for Business		
5	Existing Solutions Summary	75
6	Cybersecurity Business Goals and Stories Around Them	97
7	Communication, Communication, Communication	105
 Part III Future Threats and Solutions		
8	Future Threats	117

9	Future Solutions	125
10	Social and Ethical Aspects	137
 Part IV Cybersecurity: The New Frontier		
11	The Next-Generation Cybersecurity	145
12	Navigating a Safe Space	151
13	The Twelve Principles of Safe Places	171
14	In Place of a Conclusion	199
	References	201
	Index	223

About the Authors

Ganna Pogrebna is Professor of Behavioral Economics and Data Science at the University of Birmingham and Fellow at the Alan Turing Institute. Blending behavioral science, computer science, data analytics, engineering, and business model innovation, Ganna helps businesses, charities, cities, and individuals to better understand why they make the decisions they make and how they can optimize their behavior to achieve higher profit, better (cyber)security, more desirable social outcomes, as well as flourish and bolster their well-being. She is interested in analyzing individual and group decision-making under risk and uncertainty (ambiguity) using laboratory experiments, field experiments and non-experimental data (specifically, large non-experimental datasets). She studies how decision-makers reveal their preferences, learn, co-ordinate, and make trade-offs in static and dynamic environments. Her work aims to develop quantitative models capable of describing and predicting individual and group behavior under risk and uncertainty. Using an algorithmic approach, Ganna works on hybrid models at the intersection between decision theory and machine learning (particularly, Anthropomorphic Learning). Her recent projects focus on smart technological and social systems, cybersecurity, AI, human-computer interaction (HCI), human-data interaction (HDI), and business models. Ganna is one of the authors of the Cyber Domain-Specific Risk Taking scale (CyberDoSpeRT), a tool which allows practitioners to construct behavioral segmentation in order to design cybersecurity solutions, and which received the Organizational Psychology Award from the British Academy of Management in 2018. Her work on risk modeling and understanding human behavior under risk and uncertainty was published in highly

reputable peer-refereed academic journals and recognized by numerous awards, including the Leverhulme Fellowship Award as well as the Economic and Social Research Council/the Alan Turing Institute Fellowship Award. Since 2002, Ganna has used her expertise to develop practical solutions for businesses as a consultant.

Mark Skilton is Professor of Practice in Information Systems and Management at Warwick Business School, the University of Warwick, UK. He has over 30 years' experience as a professional consultant with a track record in the top 1000 companies in over 20 countries and across multiple public, private, and start-up sectors. He is also currently a member of the senior executive team as Head of the Applied Research and Collaboration Labs (ARC) UK at Enzen, an international energy and utility consultancy based in the UK, India, the EU, Australia, and North America. He has direct industrial experience of commercial practice leadership, boardroom, and investor strategy to program team and transformation management at scale. Mark has previously published two international practitioner books on building the digital enterprise and digital ecosystem architectures. He is a recognized international thought leader in digital, IoT, automation and AI, cyber-physical systems, cybersecurity, company strategy, telecoms, digital markets and M&A strategies, CxO practices, and technology governance. His work and views have been published in the *Financial Times*, *New York Times*, *Wall Street Journal*, *Washington Post*, *New Scientist*, *Nature*, and *Scientific American*, by Bloomberg and the Associated Press, and on many TV and radio channels around the world, including the BBC, Sky, ITV, Al Jazeera, and many others. Mark has an MBA and postgraduate qualifications in Production Engineering, Design Management, and Material Sciences from the University of Warwick, the University of Cambridge, and the University of Sheffield, UK, respectively.

Notes on Advisors

Debi Ashenden is Professor of Cyber Security in the School of Computing at the University of Portsmouth. Debi was previously Head of the Centre for Cyber Security at Cranfield University at the Defence Academy of the UK. Before becoming an academic, she was a Managing Consultant at QinetiQ (formerly DERA) and has worked in cybersecurity since 1998. Debi holds a Ph.D. in Computer Science from UCL, an M.B.A., M.Sc. in Computer Science, M.A. in Victorian Literature and B.A. (Hons) in English Literature. She has worked extensively across the public and private sector for organizations such as the UK Ministry of Defence (MoD), UK Cabinet Office, UK Home Office, Euroclear, Prudential, Barclaycard, Reuters, and Close Bros. Debi has had a number of articles on cybersecurity published, presented at a range of conferences and co-authored a book for Butterworth-Heinemann, *Risk Management for Computer Security: Protecting Your Network and Information Assets*.

Jon Crowcroft is the Marconi Professor of Communications Systems, Computer Laboratory, University of Cambridge, UK. He is also Associate Fellow of the Centre for Science and Policy and Fellow at the Alan Turing Institute, UK. Jon Crowcroft joined the University of Cambridge in 2001, prior to which he was Professor of Networked Systems at UCL in the Computer Science Department. He is a Fellow of the Royal Society, Fellow of the Association for Computing Machinery, a Chartered Fellow of the British Computer Society, a Fellow of the Institution of Electrical Engineers and a Fellow of the Royal Academy of Engineering, as well as a Fellow of the Institute of Electrical and Electronics Engineers. He was a member of

the Interactive Advertising Bureau (1996–2002) and went to the first 50 meetings of the Internet Engineering Task Force; was General Chair for the ACM SIGCOMM (1995–1999) and was a recipient of the SIGCOMM Award in 2009. He is the Principal Investigator in the Computer Lab for the EU Social Networks project, the Horizon Digital Economy project, funded by the Engineering and Physical Sciences Research Council and hubbed at Nottingham, and the EPSRC-funded federated sensor networks (i.e., sensor nets) project FRESNEL, in collaboration with Oxford, along with a new five-year project towards a Carbon Neutral Internet with Leeds. Jon has made major contributions to a number of successful start-up projects, such as the Raspberry Pi and Xen. He has been a member of the Scientific Council of IMDEA Networks since 2007. He is also on the advisory board of the Max Planck Institute for Software Systems. Jon has written, edited, and co-authored a number of books and publications which have been adopted internationally in academic courses, including *TCP/IP and Linux Protocol Implementation: Systems Code for the Linux Internet*, *Internetworking Multimedia* (2001) and *Open Distributed Systems* (1995). Jon's research interests include communications, multimedia, and social systems, especially Internet related.

Anthony Phipps is a Senior Manager leading the Digital Cyber Research team at one of the largest financial institutions in Europe. Tony started his career as an engineer and has worked in a variety of fields including electrical and electronic engineering, and, more recently, information technology. For the last 20 years he has specialized in information, cyber and physical security. He obtained his first degree in Electrical and Electronic Engineering from the University of Greenwich in 1997 and a Master's degree from the University of Westminster in Information Technology Security in 2002. He is currently working towards obtaining a Ph.D. in cybersecurity.

Haydn Povey is a CEO and Founder of Secure Thingz Inc. He is also a board member of the IoT Security Foundation. He is a recognized international expert in IoT security development. Prior to establishing Secure Thingz, he spent ten years at ARM as Director of Marketing of Security across industry sectors and in the Processor Division and product management. Secure Thingz is a provider of advanced security solutions for embedded systems in the Internet of Things. It was founded by Haydn in 2016 and recently sold to IAR Systems AB, a Swedish developer of embedded systems tools, for £20 million. The company's Secure Deploy™ architecture has been developed to solve the major security issues challenging the IoT. It claims that its solutions ensure a cost-efficient root of trust in low-cost

microcontrollers to deliver a core set of critical services through the product lifecycle, alongside a secure deployment, production, and update infrastructure in the field of embedded trust.

Karen Renaud is Professor of Cybersecurity, Division of Cybersecurity, at the Abertay University, Professor Extraordinarius at the University of South Africa, Fulbright Cyber Security Scholar 2016/2017, as well as Honorary Research Fellow (Computing Science) at the University of Glasgow, UK. Karen is a graduate of the universities in Pretoria, South Africa, and Glasgow, UK. Her main research interest is Usable Security. She publishes widely in this area and collaborates with academics in the UK, South Africa, and Canada. She also has interests in email usage in organizations, electronic voting, and technology acceptance, specifically with respect to learning support systems. Karen's research interests include the usability of security systems, graphical authentication mechanisms, security and email acceptable-use policies, the use of technology in organizations, electronic voting, and privacy. She has written many academic publications in the field of security, along with numerous book contributions, and is a frequent speaker at cybersecurity conferences.

Boris Taratine is a passionate visionary and an influential ambassador of cybersecurity and cyberdefense. He has worked for world-renowned companies across the globe, holding different senior cyber and information security technical and leadership roles, was engaged in consulting with numerous organizations and is an active participant in various industry and law enforcement forums influencing global cybersecurity development. He is a frequent speaker at various industry events. He serves as a Strategic Executive Advisor to CEOs and a member of advisory boards to new cybersecurity start-ups. Boris has nearly 30 years' experience in the cybersecurity, information security, and information technology fields, spanning different industries. He possesses extremely strong analytical and problem-solving skills and is able to find and integrate complex solutions consistent with the customer and regulatory requirements. Boris is the author of six scientific publications and nine patents (including four granted under the NATO HiTech project), and has dozens of patents pending. He is a Ph.D. candidate and graduated from the Saint-Petersburg State University with the highest honor.

Maria Vello is a CEO of the Cyber Defence Alliance (CDA). She joined the CDA in April 2016. Prior to this, she was the CEO and President of the NCFTA (National Cyber-Forensics and Training Alliance) for three years.

Before her appointment as CEO and President, Maria served on the Board of Directors of the NCFTA from its inception in 2002 to 2012, and as the Board Secretary at the NCFTA for four years. Under Maria's leadership, the NCFTA weathered several significant cyber storms (e.g., those instigated by Gameover Zeus and Darkode), playing an instrumental role in major successes across cybersecurity industry and in law enforcement. During her leadership, in 2014, the NCFTA was named in the President Obama's Executive Order. Maria was the constant driving force for the NCFTA's growth in revenues and reach. She also helped ensure the increase in the number of cybercriminal arrests as well as cases taken on by the law enforcement partners. Maria brings a wealth of experience in trust-based collaboration and information sharing across businesses in different industries. She often acts as an ambassador linking businesses with law enforcement, government and academia to proactively detect, protect, deter, dismantle, and stop cybercrime and cyberthreats. She has effectively led multinational teams to leverage cross-sector resources and threat intelligence in order to more efficiently analyze, correlate, and attribute critical real-time intelligence against emerging cyberthreats as well as to deliver actionable intelligence to both industry and law enforcement.

With more than 25 years' experience in the security, design, integration, risk, architectural design, and implementation of global corporate systems, security architectures, and networks, Maria has been responsible for integrating security best practices, risk, and compliance, as well as raising awareness at every level in every organization for which she has worked. Maria managed a Fortune Global 100 network infrastructure and systems from security, LAN, WAN, Voice, Video, Voicemail, gateways to network architecture. She was the owner of network security and vulnerability assessment company and worked for Cisco Systems in security for 7 years. Maria has been recognized as a leading expert in security throughout her career. She received the AT&T Leaders Council Award, finishing in the top 2% of the AT&T expert rankings and was the number one Regional Manager in Security while she worked for Cisco Systems. She was also honored by the FBI Executive team within the FBI Cyber Unit, Department of Justice, and the FBI Cyber Initiative Resource and Fusion Unit (CIRFU) for her exemplary service, partnership, and contributions with the Cyber Division. In 2014, she was named one of the top ten Women in Cloud. Maria received her Bachelor's degree from Duquesne University, Pittsburgh, Pennsylvania, and studied further at the Massachusetts Institute of Technology and the University of Pennsylvania's Wharton School of Business. She has also attended numerous executive leadership and management training courses,

including the Carnegie Mellon University Software Engineering Institute's certification program in the delivery, facilitation, consulting, and training of the Institute's OCTAVE methodology. In addition to being a Certified Information Systems Security Professional (CISSP), Maria also has the RAM-W physical security certification for the water industry.

Tim Watson is the Director of the Cyber Security Centre at Warwick Manufacturing Group (WMG) within the University of Warwick. With more than 25 years' experience in the computing industry and in academia, he has been involved with a wide range of computer systems on several high-profile projects and has acted as a consultant for some of the largest telecoms, power, and oil companies. He is an advisor to various parts of the UK government and to several professional and standards bodies. Tim's current research includes EU-funded projects on combating cybercrime and research into the protection of infrastructure against cyberattack. He is the Vice President (Academia) of the Trustworthy Software Initiative, a UK government-sponsored project to make software better, and a key deliverable of the UK National Cyber Security Programme. Tim is also a regular media commentator on digital forensics and cybersecurity.

Sir Alan Wilson is a current Executive Chair of the Ada Lovelace Institute, a former CEO of the Alan Turing Institute and Professor of Urban and Regional Systems in the Centre for Advanced Spatial Analysis at UCL. He is Chair of the Home Office Science Advisory Council. Alan is a Cambridge Mathematics graduate and began his research career in elementary particle physics at the Rutherford Laboratory. He turned to the social sciences, working on cities, with posts in Oxford and London before becoming Professor of Urban and Regional Geography in Leeds in 1970. He was a member of Oxford City Council from 1964 to 1967. In the late 1980s, he was the co-founder of GMAP Ltd, a university spin-out company. He was Vice Chancellor of the University of Leeds from 1991 to 2004, when he became Director-General for Higher Education in the then DfES. After a brief spell in Cambridge, he joined UCL in 2007. From 2007 to 2013, he was Chair of the Arts and Humanities Research Council; and from 2013 to 2015, he was Chair of the Lead Expert Group for the Government Office for Science Foresight on The Future of Cities project. His research field covers many aspects of the mathematical modeling of cities and the use of these models in planning. These techniques are now in common use internationally—including the concept of entropy in building spatial interaction models, summarized in *Entropy in Urban and Regional Modelling* (reissued in 2011 by Routledge). These models have been widely used in areas such

as transport planning, demography, and economic modeling. Alan's recent research focused on the applications of dynamical systems theory in relation to modeling the evolution of urban structure in both historical and contemporary settings. This led to the laying of the foundations of a comprehensive theory of urban dynamics described in *Complex Spatial Systems* (2000). He has published over 200 papers and his recent books include *The Science of Cities and Regions* (2012), his five-volume *Urban Modelling* (2012, edited), *Explorations in Urban and Regional Dynamics* (2015, with Joel Dearden), *Global Dynamics* (2016, edited), and *Geo-mathematical Modelling* (2016, edited). Alan has a particular interest in interdisciplinarity and published *Knowledge Power* in 2010; he also writes the *quaestio* blog (www.quaestio.blogweb.casa.ucl.ac.uk).

Karen Yeung is the University of Birmingham's first Interdisciplinary Chair, taking up the post of Interdisciplinary Professorial Fellow in Law, Ethics, and Informatics in the School of Law and the School of Computer Science in January 2018. She has been a Distinguished Visiting Fellow at Melbourne Law School since 2016. Together with Andrew Howes and Ganna Pogrebna, she informally leads a group of over 90 researchers at the University of Birmingham from a wide range of disciplines under the theme of *Responsible Artificial Intelligence*. Karen is actively involved in several technology policy and related initiatives in the UK and worldwide, including initiatives concerned with the governance of AI, which is one of her key research interests. In particular, she is a member of the EU's High Level Expert Group on Artificial Intelligence (since June 2018), as well as a member and rapporteur for the Council of Europe's Expert Committee on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT). Since March 2018, she has been the ethics advisor and member of the Expert Advisory Panel on Digital Medicine for the Topol Independent Technology Review for the NHS. Between 2016 and 2018, she was Chair of the Nuffield Council on Bioethics Working Party on Genome Editing and Human Reproduction. During this period, she was also a member of the World Economic Forum Global Future Council on Biotechnology. Her recent publications include *The Oxford Handbook of Law, Regulation and Technology* (2017, co-edited with Roger Brownsword and Eloise Scotford), and the Royal Society/British Academy report *Data Management and Use: Governance in the 21st Century* (2017). She is qualified to practice as a barrister and solicitor at the Supreme Court of Victoria (Australia), having completed a brief stint in professional legal practice. Karen is on the editorial boards of *Big Data & Society* and *Public Law*. As