

EAI/Springer Innovations in Communication and Computing

Shishir Kumar Shandilya

Agni Datta

Yash Kartik

Atulya Nagar

Digital Resilience: Navigating Disruption and Safeguarding Data Privacy

 **EAI**
RESEARCH MEETS INNOVATION

 Springer

EAI/Springer Innovations in Communication and Computing

Series Editor

Imrich Chlamtac, European Alliance for Innovation, Ghent, Belgium

The impact of information technologies is creating a new world yet not fully understood. The extent and speed of economic, life style and social changes already perceived in everyday life is hard to estimate without understanding the technological driving forces behind it. This series presents contributed volumes featuring the latest research and development in the various information engineering technologies that play a key role in this process. The range of topics, focusing primarily on communications and computing engineering include, but are not limited to, wireless networks; mobile communication; design and learning; gaming; interaction; e-health and pervasive healthcare; energy management; smart grids; internet of things; cognitive radio networks; computation; cloud computing; ubiquitous connectivity, and in mode general smart living, smart cities, Internet of Things and more. The series publishes a combination of expanded papers selected from hosted and sponsored European Alliance for Innovation (EAI) conferences that present cutting edge, global research as well as provide new perspectives on traditional related engineering fields. This content, complemented with open calls for contribution of book titles and individual chapters, together maintain Springer's and EAI's high standards of academic excellence. The audience for the books consists of researchers, industry professionals, advanced level students as well as practitioners in related fields of activity include information and communication specialists, security experts, economists, urban planners, doctors, and in general representatives in all those walks of life affected ad contributing to the information revolution.

Indexing: This series is indexed in Scopus, Ei Compendex, and zbMATH.

About EAI - EAI is a grassroots member organization initiated through cooperation between businesses, public, private and government organizations to address the global challenges of Europe's future competitiveness and link the European Research community with its counterparts around the globe. EAI reaches out to hundreds of thousands of individual subscribers on all continents and collaborates with an institutional member base including Fortune 500 companies, government organizations, and educational institutions, provide a free research and innovation platform. Through its open free membership model EAI promotes a new research and innovation culture based on collaboration, connectivity and recognition of excellence by community.

Shishir Kumar Shandilya • Agni Datta •
Yash Kartik • Atulya Nagar

Digital Resilience: Navigating Disruption and Safeguarding Data Privacy

 Springer

 **EAI**
RESEARCH MEETS INNOVATION

Shishir Kumar Shandilya
School of Data Science and Forecasting
Devi Ahilya Vishwavidyalaya (DAVV)
Indore, Madhya Pradesh, India

Yash Kartik
SECURE - Center of Excellence in Cyber
Security
VIT Bhopal University
Bhopal, Madhya Pradesh, India

Agni Datta
SECURE — Centre of Excellence in Cyber
Security
VIT Bhopal University
Bhopal, Madhya Pradesh, India

Atulya Nagar
School of Mathematics, Computer Science
and Engineering
Liverpool Hope University
Liverpool, UK

ISSN 2522-8595 ISSN 2522-8609 (electronic)
EAI/Springer Innovations in Communication and Computing
ISBN 978-3-031-53289-4 ISBN 978-3-031-53290-0 (eBook)
<https://doi.org/10.1007/978-3-031-53290-0>

© European Alliance for Innovation 2024

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, expressed 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.

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

Paper in this product is recyclable.

It doesn't matter how beautiful your theory is, it doesn't matter how smart you are. If it doesn't agree with the experiment, it's wrong.

Richard Phillips Feynman

To my lifelines, Smita, Samarth, and Nityaa

Shishir

*To my precious mummum and daddy who are
forever young in mind and soul, my dearest
and irreplaceable sister, and to the one who
has departed*

Agni

To my dearest parents and beloved brother

Yash

*To Jyoti, and lovely daughters, Kopal and
Priyel.*

Atulya

Preface

Audere est faucere.

Scope

The goal of the book is to provide readers with a detailed exploration of the concepts regulating digital resilience as well as their practical applications in reducing technological disruptions. The principal objective of this book, which covers a various issues related to digital infrastructure, cybersecurity, and approaches for encouraging flexibility and resilience, is to provide readers with the knowledge and abilities required for understanding and implementing the subject matter of digital resilience in life. This contribution is expected to provide significant value to a large target audience, including a diverse demography of individuals, including those enrolled in undergraduate and postgraduate programmes. It is not only designed for students seeking academic degrees in computer science, engineering, cybersecurity, information technology, and related fields. It is also relevant to professionals working in information technology (IT), cybersecurity, system administration, and technology management.

The ideas given in the book provide novel views and practical solutions for enhancing the resilience of digital systems and infrastructure inside businesses. The detailed examination of digital resilience concepts presented here has the potential to greatly improve the understanding and comprehension of students and researchers working in the fields of cybersecurity, digital infrastructure, and technology management. This fundamental knowledge, in turn, serves as a platform for informing and directing future research activities in these particular fields. Individuals entrusted with developing technology policies and regulations, in particular, stand to gain practical insights into the need for digital resilience in ensuring the security and stability of critical infrastructure.

Because of its thorough coverage, this material is highly recommended for use in beginning cybersecurity courses and other information security (infosec) instructional programmes. It offers a detailed examination of key ideas and strategies relevant to the disciplines of cybersecurity and information security, while acting as an essential primer for students beginning a cybersecurity study, providing a solid and basic reference to complete their educational requirements.

Motivation

This book examines how closely connected both domains are as a complete resource for people with a strong interest in cybersecurity, as well as students and professionals seeking assistance on the issue of digital resilience. Originally conceived as a study on digital resilience, it became apparent that any book addressing this subject would explain the field of cybersecurity due to the link between the two. Due to the COVID-19 pandemic, there has been a collective adaptation leading to the adoption of several new behavioural patterns. However, with the wide diversity of threats and the availability of potential bad actors, a flexible policy is required to ensure that our safety while using the Internet is not compromised. The concept of digital resilience is therefore broken down and examined in great detail, providing a tool that can assist individuals, communities, and even entire societies in coping with the numerous dangers present in our lives when we are online.

The challenges posed by cyber threats are numerous, including hackers purposefully breaking into our computer systems, covert data theft schemes, and unplanned havoc in our technological infrastructure by natural disasters. Broadly speaking, the dangers faced in the digital world present us with a unique and diverse set of challenges that cannot be dealt with by a singular set of plans but rather require a more comprehensive approach. Hence in this regard, the concept of digital resilience is similar to a protective barrier, equipping us with the resources necessary to bounce back fast from failures and the tenacity to persevere in the face of challenges. It provides us with the same kind of determination in the electronic domain that we possess in the physical sphere.

Maintaining an awareness of digital resilience is emerging as a critical method to protect our digital life against the rising frequency of cyberattacks, data breaches, and associated risks. As a result, the primary emphasis of this book is on investigating the numerous aspects that contribute to digital resilience. Understanding its subtleties gives us the tools we need to increase our electronic involvement and digital lives in the face of growing threats. Recent technology breakthroughs have enabled us to see first-hand the enormous potential of digital resilience. This barrier acts as a protective addition having an impact that extends beyond its immediate users to include enterprises and the broader social environment. The consequence of digital resilience in our everyday lives cannot be emphasized, and this book is an essential resource for specialist audiences wanting a thorough grasp of the problem.

The intelligent computers, the learning machines, and a one-of-a-kind digital system known as blockchain are the ones who are in charge of this digital universe. These smart innovations can detect and avoid problems in real time, which is a huge advantage. This is the equivalent, in the world of digital technology, of having a team of superheroes at your command. These technical pioneers are paving the way for a new future in which we can head off problems before they become more serious. Regardless, digital resilience is a lot more than just a technical definition. It is constructed in the shape of a wall that encircles and safeguards all of society. By adopting what is called a 'digitally resilient' mindset, individuals, corporations, and even society as a whole can strengthen their defences against the numerous online threats that are currently present. We enhance our capacity to mitigate the adverse consequences of cyberattacks, such as financial instability and disruptions to the social order, by possessing such resilience.

However, the scope of digital resilience extends well beyond simple repair; it also develops confidence in the stability of the regenerative capabilities of the digital environment. This sense of safety acts very similarly to a safety net for us while we are navigating the virtual world. The effects of digital resilience are far-reaching, penetrating not only the technological but, crucially, the social and economic underpinnings of our society as well. As the power of the digital economy continues to develop, it is important to keep in mind two required factors: innovation and growth. In this context, digital resilience functions as a catalysing force, making it possible for these components to develop to their maximum potential. In a similar vein, the complex social framework, which is driven by the interaction of a great number of distinct pieces, necessitates the presence of this power.

Digital resilience serves as a cornerstone, somewhat in the same way that a solid foundation does, and it is essential to the symbiotic relationship between the dynamics of society. The capability to recover quickly from technological setbacks is necessary for ensuring that everything works together without any difficulties. Its influence is felt not only in the technology but also in the larger social picture, where it acts as an essential variable in promoting both collaborative advancement and cohesive functionality. Its influence is felt not only in technology but also in the larger social picture. Within the pages of this academic initiative, we have all come together to emphasize how important it is to establish digital resilience.

The increasing level of sophistication in technology and the complexities of the Internet world make digital resilience an important problem. Our investigation takes a comprehensive and intellectual approach, exploring the potential of novel concepts. As we explain the many strands that contribute to the significance of digital resilience, we will conduct comprehensive research across different sectors to shed light on the numerous ways in which it influences a variety of elements. Ultimately, we aim to gain a better understanding of why digital resilience is critical in today's society and encourage its widespread adoption. We expect this book to act as a guide to the components of digital resiliency, highlighting its prevalence in the world of technology and its relevance.

Prerequisites

To fully engage with and comprehend the content of this book, readers must possess a set of essential prerequisites. These prerequisites contain a fundamental grasp of technological principles, including computer systems, networks, and software. Acquiring this level of proficiency is considered necessary for readers to understand the concepts and principles elaborated in this book. To understand the chapter related to quantum computing, readers must possess a requisite level of mathematical proficiency. While not mandatory, proficiency in fundamental mathematical principles, including algebra and statistics, is welcome in this context. The utilization of mathematical formalism is evident in very few specific sections of the book, necessitating readers to be adequately equipped to understand and interact with these mathematical components. However, it is worth noting that most readers who have taken introductory discrete mathematics or mathematics for computer science classes should be able to follow along without any issues.

While not obligatory, possessing a certain level of familiarity with cybersecurity ideas and practices might provide a significant benefit. A foundation of previous knowledge will enhance the grasp of specific chapters that explore subjects related to cybersecurity. It is expected that readers will maintain critical thinking and problem-solving abilities. The book promotes active involvement by using case studies, and reflection. The acquisition of these skills will be important for the proficient application of the principles explained to readers who possess a genuine curiosity about delving into the cross-disciplinary aspects of digital resilience. This concept spans a range of disciplines, including economics, technology, psychology, and policy design. Developing a proclivity for understanding the links and collaborative contributions of numerous fields to digital resilience will boost the reader's engagement with the book.

Pedagogy

The present book is structured into eight chapters, each of which is devoted to a specific piece of the digital world, with the aim of providing an all-round and tailored instructional approach for diverse audiences, while ensuring clarity and coherence throughout the entire book. It is worth noting that the chapters contained in this book are arranged in a deliberate and logical order, such that they encompass the constantly evolving field of computer science and technology. Each of these chapters serves as a reminder of the global significance of digital resilience and cybersecurity. What is particularly noteworthy about the structure of the book is that it has been designed to accommodate a range of teaching techniques, catering to readers of varying levels of expertise, thereby aligning with the book's primary purpose of serving as a guide to the recent developments in computer science. Besides, each chapter of the book offers an in-depth breakdown of the concepts

and phenomena that shape the digital world, while simultaneously emphasizing the complex relationship between digital resilience and cybersecurity, and highlighting their combined significance. This emphasis on their intersection enhances readers' understanding of how these distinct dimensions interact and reinforce one another.

The pedagogical structure of this text has been carefully crafted to facilitate a broad understanding and practical application of digital resilience principles. To achieve this, the book starts by laying a solid foundation in the fundamental concepts relating to digital resilience, introducing the reader to the essential concepts of digital infrastructure, cybersecurity, and adaptability, and, where necessary, presenting mathematical models and formal definitions to clarify these ideas. The pedagogical structure of the book follows a logical progression from basic to advanced topics, with each chapter building on the previous one's content, ensuring a continuous learning journey. To illustrate the applicability of digital resilience principles, the book includes case studies from the real world, which are analysed, enabling readers to apply their theoretical understanding to practical scenarios.

The book's interdisciplinary perspective is another distinguishing feature of its approach to education. To explain the essence of digital resilience, the book draws on a range of disciplines, including computer science, engineering, applied economics, and applied psychology. The implementation of digital resilience strategies in practice is a central focus of this book, and to facilitate hands-on learning, the book guides readers through the process of applying these principles and methodologies to real-world situations. The structure of the book is designed to accommodate varying levels of curiosity and expertise, as readers can select which chapters to read first after the introductory chapter, maximizing their initial time investment, while more complex portions can be deferred until later, allowing for a thorough but idiomatic understanding.

Indore, India
Bhopal, India
Bhopal, India
Liverpool, UK

Shishir Kumar Shandilya
Agni Datta
Yash Kartik
Atulya Nagar

Acknowledgement

We humbly believe that saying ‘thank you’ is a better way to show our gratitude for someone’s assistance than just acknowledging it, so that is what we will try to do. Our expertise in cybersecurity and digital resilience has been honed through the teachings and mentorship of Dr Shishir Kumar Shandilya, our co-author and mentor whom we were fortunate enough to meet during our graduate studies. He has guided and instructed us throughout the entire process of writing this book, providing invaluable support and insights. We are grateful for his constant and kind guidance, and his input has undoubtedly been a significant contributor to the book’s success.

Our journey began on a freezing winter night in our dormitory room, where we engaged in a collaborative brainstorming session with our co-authors. It was an interactive session that eventually led to the creation of a textbook and several other initiatives. We would like to take this opportunity to express our deepest gratitude to the numerous individuals who contributed significantly to the production of this book. Their valuable input and ideas have helped us to bring this project to fruition. We are mindful of the importance of not causing any kind of offence and, therefore, wish to explicitly acknowledge every individual who contributed to the project’s success. We have made a conscious effort to avoid overlooking anyone and want to express our appreciation to all those who have helped us accomplish our objectives.

We would like to express our deep gratitude towards the individuals who played a key role in the publication of our work. Eliska Valková deserves a special mention for her persistent and invaluable assistance in the process of editing and production, as well as for keeping us on track with the deadlines. Professor Imrich Chlamtac deserves major recognition for his significant contributions and innovative ideas that have not only enriched the project but also several other fields of computer science. We are truly grateful to him for his immense support. Lastly, we would like to extend our heartfelt appreciation to all the people who were essential in the successful creation of this textbook. Their contributions have been key in making this project a success.

It is important to acknowledge the help and leadership that Kadhambari S. Viswanathan, Assistant Vice President of VIT Bhopal, has consistently provided.

We would also like to express our deep appreciation and gratitude to the Chancellor, Vice President, Trustees, and Vice Chancellor of VIT Bhopal University. Further, we would like to thank our research collaborators, Ajit Kumar, Gaurav Choudhary, David (Bong Jun) Choi, Saket Upadhyay, and Chirag Ganguli, for their significant contributions to this project and other research initiatives we have collaborated on.

It is with utmost gratitude and appreciation that we express our deepest thanks to our parents, loved ones, friends, and colleagues whose encouragement and invaluable contributions have been vital in our personal and professional growth, and without whom we would be nothing more than a mere shadow of ourselves. We are particularly grateful to the dedicated research team at SECURE – Centre of Excellence (CoE) in Cyber Security, VIT Bhopal University, which we are a part of, and of which we feel privileged and honoured to be members, for their tireless efforts and commitment to excellence in the field of cybersecurity.

The students enrolled in the cybersecurity and digital forensics programme at VIT Bhopal University are deserving of special recognition for their vibrant and intellectually stimulating opinions, as well as their genuine interest in the subject matter being discussed. We extend our sincere gratitude to everyone who contributed to the identification and resolution of errata and typographical errors, including but not limited to the valuable intellectual assistance of Devangana Sujay A. and Sidharth Panda, two of our close friends and colleagues on the SECURE-CoE team, whose support and mentorship have been an integral part of our journey.

Their dedication and commitment to excellence in the field of cybersecurity have been an inspiration to us, and we are proud to be a part of this esteemed institution. We are grateful for the opportunities that we have been afforded at VIT Bhopal University, and we look forward to continuing our journey of discovery and innovation in the field of cybersecurity, thanks to the support and mentorship of our colleagues and mentors on the SECURE-CoE team. We remain determined to the quest for excellence in the field of cybersecurity and to make a beneficial contribution to the community through our research.

As we reflect on the process of creating this book, we are filled with immense gratitude towards the creators of L^AT_EX, the honourable Donald E. Knuth and Leslie Lamport, whose clever creation has been an inspiration to us since our undergraduate days, and has aided us in typesetting the contents of this book. We cannot overlook the integral part that Comprehensive TeX Archive Network (CTAN's) vast collection of macros and packages played in facilitating the creation of mathematical equations and other fancy compositions all while maintaining consistent formatting throughout the book.

Indore, India
Bhopal, India
Bhopal, India
Liverpool, UK

Shishir Kumar Shandilya
Agni Datta
Yash Kartik
Atulya Nagar

Contents

Part I Understanding Digital Resilience

1	What Is Digital Resilience?	3
1	Introduction	3
2	Context	5
3	What Is Cybersecurity?	6
4	History	8
5	Definition	9
	5.1 Technical Measures	11
	5.2 Operational Measures	12
	5.3 Cybersecurity Awareness	13
	5.4 Effective Incident Response	14
6	Digital Resilience and Cyber Resilience	15
7	Significance	19
8	Benefits	21
9	Challenges Encountered in Adoption	24
	9.1 Challenges in the Industries and the Business Sectors	25
	9.2 Challenges in the Education Sector and for Minors	26
	9.3 Challenges for Critical Infrastructures	27
	9.4 Challenges in the Socioeconomic Sphere	28
	9.5 Challenges on the Legal Front	29
	9.6 Challenges in the Technical Sphere	30
10	Characteristics of a Cyber Resilient Organization	31
	10.1 Seven Strategies to Improve Digital Resilience	31
11	Embracing a Digitally Resilient Future	40
12	Concluding Remarks	41
2	Achieving Digital Resilience with Cybersecurity	43
1	Introduction	43
2	Nature of Cyber Threats	44
	2.1 Motives and Tactics of Attackers	44
	2.2 Evolving Nature of Threats and Ongoing Vigilance	50

- 3 The Impact of Cyber Threats on Digital Resilience..... 51
 - 3.1 Cybersecurity in Maintaining Trust and Resilience 52
- 4 Types of Cyber Threats 53
 - 4.1 Malware 54
 - 4.2 Social Engineering 56
 - 4.3 Supply Chain Attacks 57
 - 4.4 Man-in-the-Middle 58
 - 4.5 Denial-of-Service 59
 - 4.6 Injection Attacks 60
 - 4.7 Zero-Day Vulnerabilities 61
- 5 Threat Intelligence 63
 - 5.1 Defining Threat Intelligence 64
 - 5.2 Attributes of Threat Intelligence 65
 - 5.3 Lifecycle of Threat Intelligence 66
 - 5.4 Types of Threat Intelligence 69
 - 5.5 Threat Intelligence with Machine Learning..... 70
- 6 Strategies for Building Digital Resilience 71
 - 6.1 Designing Systems with Resilience 72
 - 6.2 Enforcing Multi-layered Security Mechanisms 74
 - 6.3 Developing a Culture of Security Awareness and Resilience .. 75
- 7 Trustworthy System 76
 - 7.1 Fundamental Design Principles 77
 - 7.2 Benefits of Trustworthy Computing Systems 79
 - 7.3 Procedure 80
 - 7.4 Importance..... 81
 - 7.5 Concept of Zero-Trust Systems 84
 - 7.6 Advantages of Zero-Trust Systems..... 85
 - 7.7 Drawbacks of Zero-Trust Systems 86
- 8 Balancing Security and Resilience 87
 - 8.1 Security and Usability in Digital Systems 88
 - 8.2 Architecting Resilient Systems 89
- 9 Safeguarding Digital Assets 90
 - 9.1 Value of Digital Assets and Impact of Loss or Compromise... 90
- 10 Role of Encryption in Safeguarding Digital Assets 91
 - 10.1 Homomorphic Encryption 91
 - 10.2 Zero-Knowledge Proof 94
 - 10.3 Multi-party Computation 96
- 11 Enhancing the Robustness of Digital Assets 98
 - 11.1 Robust Access Controls and Authentication Protocols..... 98
 - 11.2 Safeguarding Data Through Backup Strategy 99
- 12 Incident Response 101
 - 12.1 Digital Forensics and Incident Response (DFIR)..... 103
 - 12.2 Advantages of Incident Response 106
 - 12.3 Disadvantages of Incident Response 109

- 13 Digital Resilience Through Effective IRP 110
 - 13.1 Concrete Illustrations 110
 - 13.2 Steps Towards Designing Scalable IRPs 111
- 14 Significance of Swift Response and Recovery 112
- 15 Role of Regular Drills and Exercises 113
- 16 DevSecOps 114
 - 16.1 DevSecOps and Digital Resilience 116
 - 16.2 Advantages 118
 - 16.3 Disadvantages 119
 - 16.4 Security Challenges 119
 - 16.5 Research Avenues 120
- 17 Concluding Remarks 122

Part II Building Digital Resilience

- 3 Navigating the Regulatory Landscape 127**
 - 1 Introduction 127
 - 2 Regulations and Impact on Shaping Technology 129
 - 3 Importance of Legal Frameworks 131
 - 4 Understanding Regulatory Authorities 133
 - 4.1 Government Agencies 133
 - 4.2 Industry-Specific Bodies 135
 - 5 Adaptations for Legal Frameworks 137
 - 6 Cybersecurity and Privacy Laws, USA 139
 - 6.1 FCRA, 1970 140
 - 6.2 FERPA, 1974 141
 - 6.3 ECPA, 1986 143
 - 6.4 VPPA, 1988 144
 - 6.5 HIPAA, 1996 146
 - 6.6 COPPA, 1998 147
 - 6.7 GLBA, 1999 148
 - 6.8 CCPA, 2018 150
 - 6.9 ADPPA, 2022 152
 - 7 Cybersecurity and Privacy Laws, UK 156
 - 7.1 Computer Misuse Act, 1990 156
 - 7.2 Privacy and Electronic Communications Regulations, 2003 ... 157
 - 7.3 Investigatory Powers Act, 2016 158
 - 7.4 Payment Services Regulations, 2017 159
 - 7.5 Network and Information Systems Regulations, 2018 160
 - 7.6 Data Protection Act, 2018 161
 - 7.7 UK-GDPR, 2021 162
 - 8 Cybersecurity and Privacy Laws, Australia 163
 - 8.1 The Privacy Act, 1988 164
 - 8.2 Telecommunications Act, 1997 166
 - 8.3 Electronic Transactions Act, 1999 167

8.4	Spam Act, 2003	168
8.5	DNCR Act, 2006	169
8.6	HI Act, 2010	170
8.7	MHR Act, 2012	171
8.8	TOLA Act, 2018	173
8.9	NDB Scheme, 2018	174
9	Cybersecurity and Privacy Laws, EU	176
9.1	GDPR, 2018	176
9.2	DSA, 2022	179
9.3	DMA, 2022	180
9.4	DPF, 2023	181
9.5	AI Act, 2023	182
9.6	ePR, Expected 2023	185
10	Cybersecurity and Privacy Laws, India	186
10.1	The Information Technology Act, 2000	188
10.2	Know Your Customer, 2002	189
10.3	Information Technology (Amendment) Act, 2008	190
10.4	Information Technology Rules, 2011	192
10.5	Indian SPDI Rules for Reasonable Security Practices, 2011	193
10.6	National Cyber Security Policy, 2013	195
10.7	National Cyber Security Strategy, 2020	196
10.8	IT Rules, 2021	197
10.9	The Digital Personal Data Protection Act, 2023	198
11	Cybersecurity Regulations	200
11.1	NIST	201
11.2	ISO	202
11.3	NIST Cybersecurity Framework	203
11.4	ISO Standards	206
11.5	UKCIS Digital Resilience Framework	212
12	Digital Resilience and Regulatory Compliance	215
12.1	Intersection	216
12.2	Impact of Non-compliance	217
12.3	Benefits of Regulatory Compliance	218
13	Compliance Challenges	221
13.1	Complexity of Regulatory Landscape	223
13.2	Cross-Border Compliance Issues	225
13.3	Rapidly Changing Regulations	227
13.4	Compliance Costs	230
14	Regulatory Landscape	232
14.1	Building a Regulatory Compliance Team	232
14.2	Regulatory Risk Assessment	233
14.3	Compliance Audits and Assessments	233
14.4	Compliance Monitoring and Reporting	234
15	Conforming AI to Regulatory Frameworks	235
15.1	Safe and Effective Systems	237

- 15.2 Algorithmic Discrimination and Bias 237
- 15.3 Data Privacy 238
- 15.4 Notice and Explainability 238
- 15.5 Human Alternatives, Consideration, and Fallback 239
- 16 Concluding Remarks 239
- 4 Nurturing Resilience in Minors 241**
 - 1 Introduction 241
 - 2 Digital Environment and Cybercrimes 243
 - 2.1 Cyberbullying Against Minors 243
 - 2.2 Offensive Name-Calling 244
 - 2.3 Spreading of False Rumour 244
 - 2.4 Receiving Explicit Images Without Solicitation 245
 - 2.5 Cyberstalking 246
 - 2.6 Physical Threats 246
 - 2.7 Unauthorized Dissemination of Explicit Images 247
 - 2.8 Exposure to Inappropriate Content 248
 - 3 Digital Environment and Minors 248
 - 4 Digital Environment and Supervision 250
 - 5 Digital Environment and Guidelines 252
 - 6 Digital Environment and Government’s Role 254
 - 7 Stance of the World’s Governments 255
 - 7.1 Australia 257
 - 7.2 European Union (EU) 257
 - 7.3 India 258
 - 7.4 Japan 259
 - 7.5 The United Kingdom (UK) 260
 - 7.6 The United States of America (USA) 262
 - 8 Stance of Multinational Corporations 263
 - 8.1 Microsoft 263
 - 8.2 Apple 264
 - 8.3 Facebook 265
 - 8.4 Google 265
 - 9 Stance of Non-governmental Organizations 266
 - 9.1 ICMEC 266
 - 9.2 ASACP 267
 - 9.3 WePROTECT Global Alliance 268
 - 10 Limitations of Global Digital Resilience Frameworks 269
 - 10.1 One-Size-Fits-All Approach 269
 - 10.2 Lack of Empirical Evidence 270
 - 10.3 Rapidly Changing Technology 270
 - 10.4 Limited Parental Involvement 270
 - 10.5 Insufficient Resources 271
 - 11 Guidelines for Guardians 271
 - 11.1 Tailoring Social Media Use 272

- 11.2 Adult Monitoring and Coaching..... 272
- 11.3 Minimizing Exposure to Harmful Content..... 273
- 11.4 Combatting Cyberbullying and Hate..... 273
- 11.5 Monitoring Screen Time..... 274
- 11.6 Encouraging Social Media Literacy..... 274
- 12 Concluding Remarks 277
- 5 A Study in Attack and Breaches 279**
 - 1 Introduction 279
 - 2 Implications and Repercussions..... 280
 - 3 Ukraine Powergrid Attack, 2015..... 282
 - 3.1 Synopsis 282
 - 3.2 Ramifications..... 284
 - 4 WannaCry Attack, 2017 286
 - 4.1 Synopsis 286
 - 4.2 Ramifications..... 288
 - 5 NotPetya Attack, 2017..... 289
 - 5.1 Synopsis 289
 - 5.2 Ramifications..... 293
 - 6 Marriott Breach, 2018 294
 - 6.1 Synopsis 295
 - 6.2 Ramifications..... 298
 - 7 RockYou 2021 Breach, 2021 298
 - 7.1 Synopsis 299
 - 7.2 Ramifications..... 300
 - 8 Colonial Pipeline Attack, 2021 301
 - 8.1 Synopsis 301
 - 8.2 Ramifications..... 302
 - 9 AIIMS Ransomware Attack, 2022..... 303
 - 9.1 Synopsis 303
 - 9.2 Ramifications..... 305
 - 10 Implications of Digital Resilience 306
 - 11 Concluding Remarks 308

Part III Multidimensional Digital Resilience

- 6 Role of Artificial Intelligence and Machine Learning..... 313**
 - 1 Introduction 313
 - 2 History 314
 - 3 Defining AI and ML 316
 - 3.1 Artificial Intelligence (AI)..... 316
 - 3.2 Machine Learning (ML) and Deep Learning (DL)..... 317
 - 4 Applications..... 321
 - 4.1 Agriculture 321
 - 4.2 Autonomous Systems 324
 - 4.3 Education 326

- 4.4 Cybersecurity 329
- 4.5 Energy 332
- 4.6 Entertainment 334
- 4.7 Finance 338
- 4.8 Healthcare 341
- 4.9 Manufacturing 344
- 4.10 Weather Forecasting 345
- 5 Advancing Cybersecurity Through AI 348
- 6 Advantages and Benefits 350
 - 6.1 AI and Availability 350
 - 6.2 AI and Scalability 352
 - 6.3 AI and Accuracy 354
 - 6.4 AI and Big Data 356
 - 6.5 AI and Automation 358
 - 6.6 AI and Hazard Mitigation 360
- 7 Challenges and Considerations 361
 - 7.1 AI and Data 362
 - 7.2 AI and System Integration 363
 - 7.3 AI and Professional Competence 365
 - 7.4 AI and Creativity 367
 - 7.5 AI and Resources 370
 - 7.6 AI and Ethics 371
- 8 Explainable AI 374
 - 8.1 Application 377
 - 8.2 Advantages 380
 - 8.3 Disadvantages 381
- 9 Responsible AI 383
 - 9.1 Principles 385
 - 9.2 Application 387
 - 9.3 Advantages 389
 - 9.4 Disadvantages 392
- 10 Digital Resilience with AI 393
- 11 Concluding Remarks 396
- 7 Thriving in the Quantum Era 401**
 - 1 Introduction 401
 - 1.1 Quantum Superposition 404
 - 1.2 Quantum Entanglement 405
 - 1.3 No-Cloning Theorem 407
 - 2 Quantum Computing 410
 - 2.1 Development of Quantum Computing 411
 - 2.2 Classical versus Quantum Computing 413
 - 2.3 Challenges in Quantum Computing 414
 - 3 Qubits and Quantum Gates 415
 - 3.1 Single-Qubit Gates 417

- 3.2 Multi-Qubit Gates 419
- 3.3 Quantum Algorithms 419
- 4 Quantum Cryptography 421
 - 4.1 Lattice Cryptography 425
 - 4.2 Code-Based Cryptography 428
 - 4.3 Hash-Based Cryptography 430
 - 4.4 Isogeny-Based Cryptography 432
 - 4.5 Unbalanced Oil and Vinegar Schemes 433
- 5 Quantum Key Distribution (QKD) 434
- 6 Quantum Applications 437
 - 6.1 Quantum Machine Learning (QML) 438
 - 6.2 Computational Chemistry 439
 - 6.3 Financial Portfolio and Asset Optimization 440
 - 6.4 Industrial-Scale Logistics and Scheduling 442
- 7 Challenges and Future Prospects 443
 - 7.1 Error Correction and Scaling Quantum Systems 443
 - 7.2 Ethical and Societal Implications 445
 - 7.3 Challenges in Contemporary Cryptography 446
- 8 Dangers to Conventional Cryptography 447
 - 8.1 Factorization Problem 448
 - 8.2 Discrete Logarithm Problem 450
 - 8.3 Shor’s Algorithm 452
- 9 Concluding Remarks 456
- 8 Advancing Security and Resilience 459**
 - 1 Introduction 459
 - 2 Paradigms of Computing 461
 - 2.1 Centralized Computing 461
 - 2.2 Decentralized Computing 463
 - 2.3 Distributed Computing 463
 - 2.4 Blockchain 466
 - 3 Cloud Computing 467
 - 3.1 Cloud Security 469
 - 3.2 Advantages 471
 - 3.3 Security Challenges 473
 - 3.4 Research Avenues 475
 - 4 Hardware Security 476
 - 4.1 Significance 476
 - 4.2 Security Challenges 478
 - 4.3 Future 480
 - 5 Internet of Things (IoT) 481
 - 5.1 Advantages 482
 - 5.2 Drawbacks 483
 - 5.3 Security Challenges 484
 - 5.4 Research Avenues 485

- 6 Cyber-Physical Systems (CPS) 486
 - 6.1 Significance..... 487
 - 6.2 Challenges..... 491
 - 6.3 Research Avenues..... 493
- 7 Autonomous Systems..... 494
 - 7.1 Significance..... 495
 - 7.2 Challenges..... 496
 - 7.3 Research Avenues..... 498
- 8 Adaptive Defence..... 499
 - 8.1 Significance..... 501
 - 8.2 Security Challenges..... 503
 - 8.3 Research Avenues..... 504
- 9 Cyber-Security in an Open World: New Space..... 507
 - 9.1 Significance..... 507
 - 9.2 Security Challenges..... 508
 - 9.3 Research Avenues..... 510
- 10 Computational Psychology and Cyberpsychology..... 512
 - 10.1 Significance..... 514
 - 10.2 Ethical Considerations..... 516
 - 10.3 Psychological Factors..... 516
 - 10.4 Designing Resilient Systems..... 516
 - 10.5 Ethical Considerations..... 517
 - 10.6 Research Approaches..... 518
- 11 Consideration of Human Factors..... 519
 - 11.1 Human-Centric Approaches..... 520
 - 11.2 Recognizing Human Error and Behaviour..... 521
 - 11.3 Training and Education..... 521
 - 11.4 Interdisciplinary Collaboration..... 521
- 12 Metrics for Resilience..... 522
 - 12.1 Defining and Measuring Resilience..... 522
 - 12.2 Quantitative Metrics..... 523
 - 12.3 Qualitative Metrics..... 523
 - 12.4 Challenges in Resilience Metrics..... 524
 - 12.5 Role of Metrics in Resilience Strategies..... 525
- 13 Concluding Remarks..... 526

- Glossary..... 531**
- References..... 537**
- Index..... 553**

About the Authors

Shishir Kumar Shandilya, DSc, PhD, is an Associate Professor in the School of Data Science and Forecasting at Devi Ahilya University in India. He is also a Visiting Professor at Liverpool Hope University in the United Kingdom. He is a Cambridge University-certified professional teacher and trainer, a TEDx speaker, an Association for Computing Machinery (ACM) Distinguished Speaker, and a senior member of Institute of Electrical and Electronics Engineers (IEEE). Shandilya is a National Association of Software and Service Companies (NASSCOM)-certified master trainer for security analysts in Security Operations Center (SOC) (SSC/Q0909: National Vocational Education Qualification Framework (NVEQF) Level 7). He has received the International Development Association (IDA) Teaching Excellence Award for distinctive use of technology in teaching by the Indian Didactics Association in Bangalore (2016), and the Young Scientist Award for two consecutive years, 2005 and 2006, by the MP Science Congress and MP Council of Science and Technology. He is a highly regarded author with published research works with reputable academic publishers such as Springer, IGI-USA, River Denmark, and Prentice Hall of India. Shandilya also has international and national patents and copyrights granted for adaptive cyber defence methods. His research interest includes adaptive defence, advanced digital investigation and forensic methods, explainable artificial intelligence, privacy-preserving computing, nature-inspired cryptography (NIC), and nature-inspired cyber security (NICS).

Agni Datta is a cryptologist working with SECURE – Centre of Excellence in Cyber Security and a researcher who specializes in theoretical computer science at VIT Bhopal University in India. He is a member of several prestigious professional associations, including ACM, IEEE, American Mathematical Society (AMS), and Society for Industrial and Applied Mathematics (SIAM). His research interests include various cryptographic primitives like zero-knowledge proofs, multiparty computation, and lattice cryptography. He is particularly focused on security primitives for computing, as well as computational complexity and probabilistic proofs.

Yash Kartik is a security researcher working at SECURE – Centre of Excellence in Cyber Security at VIT Bhopal University in India. He is affiliated with esteemed organizations, such as SIAM, ACM, IEEE, and AMS. His research focuses on security methods such as cybersecurity for space systems, anonymous networking, and cyber resilience. He also has a keen interest in cryptographic primitives like zero-knowledge proofs, secure multi-party computation, and homomorphic encryption.

Atulya Nagar Foundation Professor of Computer and Mathematical Sciences at Liverpool Hope University, and Head of the Department of Computer Science, is a distinguished mathematician with expertise spanning computational science, bioinformatics, operations research, and systems engineering. Awarded a Commonwealth Fellowship, he earned his doctorate in applied non-linear mathematics from the University of York in 1996. Nagar is internationally recognized for his work in theoretical computer science, applied mathematical analysis, operations research, and industrial systems engineering. Leading the Intrusion Detection System (IDS) research group, he focuses on strategic and applied research, particularly in advancing applications of engineering, computational systems, and biological systems. The group's notable contributions include innovative DNA sequence analysis using sophisticated computational techniques. Nagar has published extensively in reputable outlets like the IEE and IEEE, and he serves on editorial boards for prestigious journals. His leadership extends to chairing and participating in international conferences. In addition to his academic roles, Nagar supervises PhD projects, serves as an external examiner, and holds visiting and adjunct professorships. His teaching expertise encompasses Applied Analysis, Systems Engineering, and Computational Biology. Before joining Liverpool Hope University, he made significant contributions as a Senior Research Scientist at Brunel University, focusing on Engineering and Physical Sciences Research Council (EPSRC)-sponsored research projects in mathematical sciences and systems engineering.

List of Figures

Fig. 1.1	Cybersecurity mindmap	8
Fig. 1.2	Digital resilience	12
Fig. 1.3	Critical infrastructure	27
Fig. 1.4	Seven-step strategy	32
Fig. 2.1	Cyber kill chain	47
Fig. 2.2	A basic firewall architecture	49
Fig. 2.3	An example of the basic types of cyber threats	54
Fig. 2.4	Categorization of malware	55
Fig. 2.5	Social engineering attack	56
Fig. 2.6	Anatomy of supply chain attacks	57
Fig. 2.7	Normal connection versus man-in-the-middle	58
Fig. 2.8	Usage of botnet in DoS	59
Fig. 2.9	Categorization of injection attacks	61
Fig. 2.10	Anatomy of zero-day vulnerability exploitation	62
Fig. 2.11	Cyber threat intelligence cycle	66
Fig. 2.12	Homomorphic encryption in cloud	92
Fig. 2.13	Zero-knowledge proof	94
Fig. 2.14	NIST incident response cycle	102
Fig. 2.15	NIST digital forensics framework	104
Fig. 2.16	DevSecOps versus DevOps	116
Fig. 6.1	AI and its domains	318
Fig. 6.2	Interrelation of XAI	375
Fig. 6.3	White box versus black box	376
Fig. 8.1	Distributive computing	464
Fig. 8.2	Blockchain	467
Fig. 8.3	Cloud computing paradigm	468
Fig. 8.4	Hardware security components	476
Fig. 8.5	IoT system	482
Fig. 8.6	Cyber-Physical Systems (CPS)	486
Fig. 8.7	Interaction of CPS	486
Fig. 8.8	Intersection of cyberpsychology with computational intelligence	514

List of Tables

Table 1.1	Cybersecurity measures for cyber resiliency [Ros+21]	18
Table 1.2	Digital resilience vs cyber resilience	19
Table 2.1	Incident response classifications	102
Table 2.2	Comparison of digital forensics and incident response	107
Table 2.3	Comparison of DevOps and DevSecOps	115
Table 4.1	Risks, guidelines, and effects of screen time	275
Table 6.1	Comparison of machine learning and deep learning	320
Table 6.2	Comparison of XAI and RAI	384
Table 7.1	Post-quantum cryptographic methods	424
Table 8.1	Comparison of centralized, decentralized, and distributed computing	462
Table 8.2	Comparison of CPS and IoT	488
Table 8.3	Computational psychology and cyberpsychology	513

Part I
Understanding Digital Resilience

Chapter 1

What Is Digital Resilience?



1 Introduction

The digital world can be compared to an expansive and interconnected ecosystem, similar to the complex balance observed among various species and organisms residing in a coral reef. The concept of digital resilience refers to the capacity of the digital ecosystem to endure and overcome unforeseen challenges. This involves the adoption of policies and safeguards designed to improve the authenticity, confidentiality, and uninterrupted operation of digital operations, similar to conservation efforts that safeguard the welfare of a coral reef. By promoting the development of digital resilience, both organizations and individuals may successfully protect the stability and flexibility of their digital systems and technologies in response to the constantly changing digital space. This phenomenon might be compared to the resilience exhibited by coral reefs, which possess the capacity to endure and recuperate from diverse disturbances.

This example serves as a significant representation of the present state of cybersecurity, emphasizing the need for individuals, enterprises, and other societal entities to possess the capacity to effectively surmount the wide range of problems associated with cyber threats in the present-day scenario. To fulfil this requirement, it is important to prioritize the development of our collective *digital resilience*. This involves the establishment and implementation of robust protocols for cybersecurity, the formulation and implementation of efficient strategies to mitigate incidents, and the development of a phase of education and consciousness surrounding cybersecurity concerns. By operating together, we can enhance our ability to face and adjust to the challenges presented by the digital age. This includes safeguarding our interests as well as the broader welfare of our communities from the risks associated with cyber threats.

The development of digital resilience presents numerous significant advantages that incorporate various dimensions of personal, organizational, and societal

domains. The seamless continuation of company operations in the face of cyber threats is an integral component of digital resilience. Economic operations can continue uninterrupted as a result of this, which helps businesses cope with digital interruptions. The development of digital resilience serves to enhance the preservation of one's reputation, which is a very valuable resource for both individuals and companies.

Similarly, the impacts of cyberattacks on critical infrastructure, a recurring issue in today's networked world, might be lessened by the construction of digital resilience. The potential negative consequences for critical social infrastructures such as power grids, transportation systems, and communication networks might be reduced by enhancing the capability to confront and recover from cyberattacks, therefore strengthening societal stability and security. The concept of digital resilience is essential in protecting the integrity and legitimacy of democratic processes. The growing use of digital platforms for elections and civic participation has raised concerns about their vulnerability to cyber manipulation, presenting a significant danger to the integrity of democratic processes. The goal of improving digital resilience is also to create a strong defensive system against malicious influences, maintaining the integrity of democratic processes.

Attaining digital resilience is contingent upon collaborative undertakings and efforts of individuals, organizations, and governmental entities. The successful execution of a strategy requires the allocation of resources towards cybersecurity tools and technology, the development of a cybersecurity-conscious culture through extensive awareness and instructional initiatives, and the facilitation of information exchange and collaborative initiatives.

Governments play a foundational role in facilitating and advancing the promotion and development of digital resilience. Government entities have the authority to adopt and enforce legislation and regulations that mark the parameters of cybersecurity practices and standards, thereby promoting a cohesive and uniform approach across various industries. It is important to recognize the role that governments play in distributing money for the progress of research and development in state-of-the-art cybersecurity measures. The implementation of this proactive approach aims to strengthen the range of strategies utilized in addressing cyber threats.

Also, the distribution of aid and resources to organizations and communities, especially in the early stages of their efforts to develop digital resilience, holds special significance. Governments are critical and integral in promoting the establishment and implementation of robust cybersecurity plans by offering support and, therefore, enabling a conducive environment for the development and execution of those initiatives. Accordingly, this facilitates firms' efficient management of and recovery from cyber disturbances.

Marking today's widespread technology integration and the increase in sophisticated cyberattacks, it is crucial to highlight the development of digital resilience. To meet this importance, stakeholders must develop and implement a strategy that comprises the development and deployment of robust cybersecurity initiatives, the establishment of effective strategies for managing cyber incidents, and the promotion of a cultural environment that prioritizes cybersecurity awareness and education.