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

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 — Shishir Kumar Shandilya
Bhopal, India — Agni Datta
Bhopal, India — Yash Kartik
Liverpool, UK — 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 LaTeX, 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 — Shishir Kumar Shandilya
Bhopal, India — Agni Datta
Bhopal, India — Yash Kartik
Liverpool, UK — Atulya Nagar

Contents

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

List of Tables

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

S. K. Shandilya et al., *Digital Resilience: Navigating Disruption and Safeguarding Data Privacy*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-031-53290-0_1

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.