THE COMPREHENSIVE GUIDE TO CYBERSECURITY CAREERS

A Professional's Roadmap for the Digital Security Age

Dr. Jason Edwards, DMIST, CISSP

J.ROSS PUBLISHING

ISBN-13: 978-1-60427-202-4
e-ISBN: 978-1-60427-855-2

Printed and bound in the U.S.A. Printed on acid-free paper.

10 9 8 7 6 5 4 3 2 1

Library of Congress Cataloging-in-Publication Data can be found in the WAV section of the publisher's website at www.jrosspub.com/wav.

Direct all inquiries to J. Ross Publishing, Inc., 151 N. Nob Hill Rd., Suite 476, Plantation, FL 33324.

Phone: (954) 727-9333
Fax: (561) 892-0700
Web: www.jrosspub.com

To Michelle, Chris, Ceylin, Mayra, and
all of my esteemed students,

This book is dedicated to you—the bright stars
of my life and the classroom.

To Michelle, Chris, Ceylin, and Mayra—you are the greatest gifts life has ever given me. Each of you, unique in your own right, has filled my heart with immeasurable joy and pride: Michelle, with your keen intellect and compassionate heart; Chris, whose resilience and creativity know no bounds; Ceylin, a beacon of determination and grace; and Mayra, whose vibrant spirit and curiosity light up every room. Together, you form a constellation of brilliance and love that guides me daily.

To my students, past, present, and future—you are the reason I am inspired to teach, learn, and grow continually. Your thirst for knowledge, diverse perspectives, and boundless potential have enriched not only my career but my life in profound ways. Each of you has left an indelible mark on my journey as an educator. I am forever grateful for the privilege of being a part of your academic and personal growth.

This book reflects my thoughts and experiences and the lessons I learned and shared with each of you. It is a mosaic of our collective journey, a testament to the power of learning, and a celebration of the bonds we have formed. May you always carry the joy of discovery, the courage to challenge the unknown, and the strength to pursue your dreams.

With most profound admiration and love,

Jason (Dad)

CONTENTS

PREFACE

Welcome to a comprehensive journey into the dynamic and ever-evolving world of cybersecurity. This book is more than just a guide; it is a companion for anyone from novices to experienced professionals who are eager to navigate the intricate landscape of cybersecurity. Our core purpose is to offer a detailed and insightful exploration of cybersecurity roles, education paths, skill requirements, and emerging trends in this critical field. Whether you are contemplating a career in cybersecurity, seeking to expand your expertise, or aiming to stay abreast of the latest developments, this book promises to be an invaluable resource in your professional journey. Join us as we delve into the multifaceted realm of cybersecurity, equipping you with the knowledge and tools necessary to thrive in this exciting and indispensable domain.

AUTHOR'S BACKGROUND IN CYBERSECURITY

My journey into the world of cybersecurity began over two decades ago, driven by a blend of curiosity and a profound sense of the critical role that digital security plays in our lives. As a current professor of cybersecurity and a seasoned veteran in this field, my experiences span various sectors, including the military, insurance, finance, technology, and energy. These diverse environments have enriched my understanding of cybersecurity challenges and highlighted this field's universal importance.

Holding key leadership positions throughout my career, I have witnessed the evolution of cyber threats and the need for robust defense mechanisms. My passion for cybersecurity extends beyond professional responsibilities, as I regularly share insights at conferences and seminars, contributing to the broader conversation on digital safety and innovation.

Academically, my foundation in Information Technology, with a Bachelor's and Master's degree, was further solidified by a Doctorate in Cybersecurity.

This academic journey, coupled with certifications like Certified Information Systems Security Professional and Certified in Risk and Information Systems Control, has equipped me with a comprehensive understanding of cybersecurity's technical and strategic aspects. This book is a culmination of my experiences, learnings, and steadfast commitment to advancing the field of cybersecurity.

MOTIVATION FOR WRITING THIS BOOK

The inspiration for this book stems from my extensive experience as a teacher and mentor in cybersecurity. Over the years I have had the privilege of instructing and guiding thousands of individuals in the classroom and through an active and vibrant LinkedIn network. This interaction with a diverse range of aspiring and established cybersecurity professionals has afforded me a unique perspective on the myriad challenges and opportunities that define this field.

I noticed a significant gap in the existing literature—the lack of a comprehensive guide that addresses the technical aspects of cybersecurity and delves into the practicalities of building a successful career in this domain. Many resources cover the *what* of cybersecurity, but there is a scarcity of literature addressing the *how* of navigating a career path in this dynamic industry. This book aims to bridge that gap by offering real-world insights, actionable advice, and a detailed exploration of various career paths, roles, and the evolving nature of cybersecurity work. It is designed to be an indispensable resource for anyone at any stage of their cybersecurity career, enriched by the lessons from my journey and the many voices I have encountered.

CHAPTER SYNOPSIS

The book is structured to provide a comprehensive and practical insight into cybersecurity. Each chapter is meticulously crafted to guide you through various facets of the field, blending educational theory with practical advice:

1. **Introduction to the Cybersecurity World:** This chapter sets the stage, offering a broad overview of the cybersecurity landscape. It addresses the fundamental concepts, current challenges, and the significance of cybersecurity in our digital era.
2. **Paths of Cybersecurity Education:** Here, we explore the different educational pathways one can pursue in cybersecurity. The chapter

emphasizes the importance of continuous learning in this rapidly evolving field, from university programs to self-study routes.

3. **Certifications and Their Significance:** Focused on the role of certifications, this chapter provides a roadmap for obtaining various cybersecurity certifications, highlighting their importance in career advancement.
4. **Personal Development and Soft Skills in Cybersecurity:** Beyond technical skills, this chapter delves into the soft skills necessary for success in cybersecurity, such as teamwork, problem-solving, and stress management.
5. **Building a Strong Portfolio:** Practical tips on creating a compelling cybersecurity portfolio are provided here. It covers everything from showcasing problem-solving skills to leveraging experiences in open-source projects and hackathons.
6. **Navigating the Cybersecurity Job Market:** This chapter offers guidance on job search strategies, resume tailoring, and interview preparation, crucial for a successful career in cybersecurity.
7. **Social Networking Strategies on LinkedIn:** The focus here is leveraging LinkedIn for career growth, including optimizing your profile and networking.
8. **Technical Roles in Cybersecurity:** An in-depth look at various technical roles in the field; this chapter helps readers understand the specific skills and responsibilities associated with each role.
9. **Management Roles in Cybersecurity:** Here, the emphasis is on leadership positions in cybersecurity, detailing roles like Chief Information Security Officer and Security Architect and the pathways to these positions.
10. **Research and Development in Cybersecurity:** This chapter highlights cybersecurity research and development roles, such as Cryptographers and Security Software Developers.
11. **Policy and Training Roles in Cybersecurity:** Focused on roles involving cybersecurity policy and training, it explores positions like Cybersecurity Policymaker and Trainer.
12. **Risk and Compliance Roles in Cybersecurity:** Covering the critical area of risk and compliance, this chapter outlines roles like Compliance Director and Information Security Auditor.
13. **Threat Intelligence Roles in Cybersecurity:** Here, we delve into the world of threat intelligence, discussing roles such as Cyber Counterintelligence Specialist and Threat Intelligence Analyst.

14. **Cloud Security Roles in Cybersecurity:** With the rise of cloud computing, this chapter focuses on roles specific to cloud security.
15. **Artificial Intelligence (AI) Roles in Cybersecurity:** This chapter explores the intersection of AI and cybersecurity, discussing roles like AI Security Analyst and Machine Learning Security Engineer.
16. **Cybersecurity Across Different Sectors:** An overview of how cybersecurity roles vary across finance, healthcare, and government sectors.
17. **Future Trends in Cybersecurity Careers:** The concluding chapter looks at the future of cybersecurity careers, discussing emerging trends, the role of AI and automation, and the importance of adaptability and continuous learning in the field.

TARGET AUDIENCE

This book is meticulously designed to cater to a wide and varied audience, encompassing individuals at different stages of their cybersecurity journey:

1. **Students and aspiring cybersecurity professionals:** This book is an essential guide for students and aspiring professionals embarking on their cybersecurity journey. It provides foundational knowledge, introduces various career paths, and offers guidance on educational routes and certifications. The early chapters are particularly beneficial for those seeking to gain a solid grounding in the basics of cybersecurity.
2. **Established cybersecurity professionals:** For professionals already in the field, this book offers advanced insights into specialized roles, emerging trends, and strategies for career advancement. Chapters focusing on management roles, sector-specific cybersecurity challenges, and future trends are particularly relevant. The book also serves as a refresher on the latest developments in cybersecurity, ensuring that established professionals stay updated in this fast-paced domain.
3. **Career changers and enthusiasts:** Individuals looking to transition into cybersecurity from other fields will find this book extremely valuable. It provides a clear roadmap for acquiring the necessary skills and credentials, making it easier for career changers to navigate this new landscape. Cybersecurity enthusiasts who may not be looking for a professional role but are keen to understand the field will also find the book informative and engaging.

4. **Academicians and trainers:** Educators and trainers in cybersecurity can use this book as a resource to enhance their curriculum. The comprehensive coverage of various roles and the latest trends in cybersecurity makes it an excellent reference for academic purposes.

RELEVANCE IN TODAY'S CYBERSECURITY LANDSCAPE

Cybersecurity is more critical than ever in today's rapidly evolving digital world. The book is acutely aligned with current trends and pressing challenges in the cybersecurity landscape:

1. **Emerging threats and technologies:** The cybersecurity domain continually faces new threats and adapts to groundbreaking technologies. This book addresses these challenges head-on, discussing the latest cyber threats like ransomware, phishing, and state-sponsored attacks. It also delves into cutting-edge technologies such as AI, Machine Learning (ML), and blockchain and their implications in cybersecurity.
2. **Increasing need for cybersecurity professionals:** With the rise in cyberattacks, there is a growing demand for skilled cybersecurity professionals. The book tackles this issue by providing guidance on entering and navigating the cybersecurity field, outlining various career paths and the skills required for each.
3. **The shift toward remote work and cloud security:** The recent shift toward remote work has brought new challenges in securing remote networks and cloud infrastructures. The book includes dedicated chapters on cloud security roles and strategies, making it a timely resource for professionals dealing with these modern complexities.
4. **Compliance and regulatory environment:** As regulations like the General Data Protection Regulation and the California Consumer Privacy Act become more prominent, understanding cybersecurity's legal and compliance aspects is crucial. This book covers these aspects, providing insights into roles like Compliance Officers and Auditors, which are essential in today's regulatory landscape.
5. **Cybersecurity in diverse sectors:** This book acknowledges that cybersecurity challenges vary across different sectors, such as finance, healthcare, and government. It provides sector-specific insights, making it relevant for professionals working in various industries.

6. **Integration of cybersecurity in business strategy:** Today, cybersecurity is not just a technical issue but a critical part of business strategy. This book covers management roles in cybersecurity, highlighting how cybersecurity knowledge is vital for business leaders and decision makers.

PRACTICAL APPLICATIONS

This book is designed to impart knowledge and serve as a practical toolkit for real-world application:

1. **Career path guidance:** The book provides detailed insights into various cybersecurity roles and paths, allowing readers to identify and pursue careers that align with their interests and skills. For example, someone interested in a technical role can follow the roadmap for becoming a Penetration Tester. At the same time, those inclined toward policy might find the pathway to becoming a Cybersecurity Policymaker more relevant.
2. **Skill development and enhancement:** Each chapter offers actionable advice on developing the necessary skills for different cybersecurity roles. Readers can apply these tips to improve their technical proficiency, soft skills, and overall understanding of cybersecurity concepts.
3. **Certification and training resources:** Recognizing the importance of certifications in cybersecurity, the book includes comprehensive lists and overviews of certifications such as Certified Information Systems Security Professional and Certified in Risk and Information Systems Control. This serves as a guide for readers to choose and pursue certifications that will enhance their career prospects.
4. **Application in diverse sectors:** The book's sector-specific insights equip readers to apply cybersecurity principles in various industries. For instance, a professional working in healthcare can utilize the healthcare cybersecurity chapter to understand and address unique challenges in their field.
5. **Practical tips for the job market and networking:** With chapters dedicated to job search strategies, resume writing, and leveraging LinkedIn for networking, readers can directly apply this advice to enhance their professional presence and increase job opportunities in the cybersecurity sector.

6. **Guidance for continuous learning:** Emphasizing the importance of lifelong learning in cybersecurity, the book provides strategies and resources for continuous education, ensuring that readers can keep pace with the rapidly evolving field.

ENCOURAGEMENT FOR CONTINUOUS LEARNING

In the dynamic and ever-changing field of cybersecurity, continuous learning is not just an advantage; it is a necessity. This book strongly emphasizes the importance of ongoing education and skill enhancement to stay abreast of the latest developments and threats in the cybersecurity landscape:

1. **Evolving cyber threats:** Cyber threats and technologies evolve at a breakneck pace, making continuous learning vital for staying effective in combating these threats. This book encourages readers to be curious, seek new knowledge, and stay informed about the latest cyber threats, security tools, and mitigation strategies.
2. **Adapting to technological advancements:** As new technologies like AI, Internet of Things, and blockchain become more integrated into our digital ecosystem, they bring new challenges and opportunities in cybersecurity. Continuous learning enables professionals to understand and adapt to these technological changes, ensuring they remain relevant and practical.
3. **Professional growth and career advancement:** The book highlights how continuous learning and upskilling can lead to career growth. By acquiring new certifications, attending workshops, and pursuing advanced degrees, professionals can open doors to higher positions, specialized roles, and broader career opportunities.
4. **Engagement with the cybersecurity community:** Networking and engagement with the cybersecurity community are pivotal for learning and growth. The book encourages readers to participate in forums, attend conferences, join professional groups, and engage on platforms like LinkedIn. This community involvement facilitates the exchange of ideas, keeps professionals updated on industry trends, and provides opportunities for collaboration.
5. **Sharing knowledge and experiences:** Continuous learning also involves sharing one's knowledge and experiences. Mentoring, contributing to discussions, and writing articles or blogs help others and reinforces the professional's understanding and perspective.

FINAL THOUGHTS AND ENCOURAGEMENT

As we conclude, I want to leave aspiring cybersecurity professionals with words of encouragement and reflection. Becoming a skilled professional in this field is challenging but immensely rewarding and critically important in our modern world:

1. **Encouragement for aspiring professionals:** Remember that your contributions are invaluable to all those who are embarking on or continuing their journey in cybersecurity. The road may seem daunting sometimes, but your persistence and dedication will pay off. Each challenge you face is an opportunity to grow; every obstacle you overcome is a step toward mastery. Cybersecurity is not just a career; it is a commitment to protecting the digital integrity and security of individuals, organizations, and nations. Your role in this field is not just a job—it is a service to the greater good.
2. **The critical role of cybersecurity:** In today's interconnected world, the importance of cybersecurity cannot be overstated. With the increasing reliance on digital infrastructure, the role of cybersecurity professionals has never been more crucial. You are the guardians of the digital frontier, the defenders against unseen threats, and the architects of safe digital spaces. Your work ensures the safety of digital information, protects privacy, and upholds the very fabric of our digital society.
3. **A call to action:** As you move forward, take the knowledge, skills, and insights gained from this book and use them to make a difference. Stay curious, remain vigilant, and continuously seek to improve your skills and understanding. Remember, in cybersecurity, you are not just building a career; you are shaping the future of digital security and, by extension, our digital world.

ACKNOWLEDGMENTS

As I reflect on the journey of writing this book, I am filled with immense gratitude toward many who have supported, inspired, and walked alongside me.

First and foremost, my heartfelt thanks to the great leaders in the field of cybersecurity. Your vision, determination, and leadership have shaped the industry and have been a guiding light in my career and the writing of this book. Your contributions have been invaluable, and your footprints in the digital sands are what many of us aspire to follow.

To the incredible friends I have made along the way—your camaraderie, insights, and endless debates have enriched this journey beyond words. Our discussions, whether in conference halls or over coffee, have been the breeding ground for many ideas on these pages. Your support and encouragement have been a constant source of motivation.

A special acknowledgment to my family—your unwavering support and understanding have been my backbone. Balancing the demands of writing with personal life is no small feat, and it would have been impossible without your patience, love, and, sometimes, sacrifices. You are my rock, and this accomplishment is as much yours as it is mine.

And last but not least, a peculiar and special thanks to the survivors of the A7 program—you know who you are. Your resilience in the face of our *unique* challenges (and yes, I am using the term *unique* as sarcastically as possible) has been both a source of inspiration and amusement. The A7 program, with all its quirks, has been a memorable chapter in my life, and you, my fellow survivors, made it all the more remarkable. Your ability to navigate the labyrinth of our shared experiences with humor and grit is nothing short of admirable.

Thank you to each of you who has been a part of this journey. Your influence has been the wind beneath this book's wings; for that, I am eternally grateful.

ABOUT THE AUTHOR

Dr. Jason Edwards is a seasoned cybersecurity expert with extensive experience across many industries, including technology, finance, insurance, and energy. His professional journey is enriched by a Doctorate in Management, Information Systems, and Information Technology, along with profound roles that have contributed to cybersecurity resilience and regulatory compliance for diverse organizations. Each role reflects Jason's depth of expertise and strategic approach, demonstrating his capability to enhance organizational cybersecurity frameworks and navigate complex risk and compliance landscapes.

A Bronze Star punctuates his remarkable 22-year career as an Army officer, a testament to his extraordinary service and dedication. Beyond organizational contributions, Jason is a stalwart in the cybersecurity community. He engages a broad audience through insightful publications on LinkedIn and steers a comprehensive cybersecurity newsletter, reaching tens of thousands of readers weekly. Jason is the author of several books and lives with his family in San Antonio, Texas.

This book has free material available for download from the Web Added Value™ resource center at *www.jrosspub.com*

At J. Ross Publishing we are committed to providing today's professional with practical, hands-on tools that enhance the learning experience and give readers an opportunity to apply what they have learned. That is why we offer free ancillary materials available for download on this book and all participating Web Added Value™ publications. These online resources may include interactive versions of material that appears in the book or supplemental templates, worksheets, models, plans, case studies, proposals, spreadsheets and assessment tools, among other things. Whenever you see the WAV™ symbol in any of our publications, it means bonus materials accompany the book and are available from the Web Added Value Download Resource Center at www.jrosspub.com.

Downloads for *The Comprehensive Guide to Cybersecurity Careers* include a Behavioral Interview Prep Guide for cybersecurity professionals.

1

INTRODUCTION TO THE CYBERSECURITY WORLD

In the ever-evolving digital landscape, cybersecurity has become a cornerstone of technological and organizational strategy. As we embark on a journey through the realm of cybersecurity, it is essential to grasp the current state of this dynamic field.

Recent cybersecurity incidents have starkly highlighted the vulnerabilities and potential impacts of cyberattacks. From large-scale data breaches affecting millions of users to sophisticated ransomware attacks crippling critical infrastructure, these incidents serve as a wake-up call to the importance of robust cybersecurity measures. The fallout from these breaches extends beyond immediate financial losses, encompassing long-term reputational damage, legal repercussions, and a shaken trust in digital systems.

The evolution of cyber threats is a testament to the ongoing arms race between cybersecurity professionals and cyber criminals. Hackers continually refine their techniques, employing advanced methods like artificial intelligence and machine learning to bypass traditional security measures. This constant progression demands an equally dynamic and proactive approach to cybersecurity, where ongoing education and adaptation are nonnegotiable.

Global cybersecurity trends reflect a growing recognition of these threats. Increased investment in cybersecurity infrastructure, the rise of cybersecurity insurance, and the implementation of stringent regulatory frameworks exemplify how nations and corporations respond to these challenges. This global perspective is crucial since cyber threats know no boundaries and can quickly ripple across countries and sectors.

The role of cybersecurity spans various sectors, each with its unique challenges and requirements. In the healthcare sector, for instance, protecting patient data is paramount, while in finance, ensuring the integrity of

transactions and financial data is critical. The public sector also faces challenges when safeguarding national security interests and citizen data. Across all these sectors, the common thread is the need for robust, tailored cybersecurity strategies to protect against the increasingly sophisticated landscape of cyber threats. See Table 1.1 for some important cyber statistics.

Table 1.1 Key cyber statistics

From	Description	Key Statistics/Details
Last decade	Data breaches worldwide	Over 300 breaches led to the loss of at least 100,000 files each.
2018	Data breaches in the United States	More than 1,200 breaches, exposing 446.5 million records.
First half of 2019	Breaches resulting in data exposure worldwide	4.1 billion exposed records were reported between January and June.
2021	Record number of breaches in the United States	1,291 breaches between January 1 and September 30, a 17% increase from 2020.
Global costs	Average data breach costs (2019)	Climbed to $3.92 million, up from $3.86 million in 2018.
Common causes	Causes of data breach incidents worldwide	48% due to employee/contractor negligence.
Business impact	Impact on businesses by data breaches	43% of incidents impact small businesses; 95% affect government organizations, retail companies, or technology companies.
Method	Standard method used in breaches	Spear phishing or targeted emails are used in 91% of successful breaches.

Sources:

1. https://www.forbes.com/sites/niallmccarthy/2014/08/26/chart-the-biggest-data-breaches-in-u-s-history/?sh=350e92807735
2. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/
3. https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/?sh=29cea594bd54
4. https://www.securitymagazine.com/articles/96667-the-top-data-breaches-of-2021
5. https://purplesec.us/resources/cyber-security-statistics/

THE IMPORTANCE OF CYBERSECURITY IN TODAY'S DIGITAL AGE

In today's digital age, the significance of cybersecurity cannot be overstated. As we increasingly rely on digital technologies for personal and professional activities, safeguarding data and systems becomes paramount.

Protecting personal and corporate data stands at the forefront of cybersecurity efforts. For individuals, personal data encompasses sensitive information such as financial records, health information, and private communications, all of which are susceptible to breaches. The consequences of such breaches can range from identity theft to financial fraud. For corporations, the stakes are equally high. Corporate data includes proprietary information, customer data, and trade secrets, which are all vital to a company's competitive edge and reputation. A breach can lead to significant financial losses, customer trust erosion, and long-term brand damage.

Ensuring business continuity is another critical aspect of cybersecurity. In an era where businesses operate in a highly interconnected digital ecosystem, a single cybersecurity incident can disrupt operations, leading to downtime and loss of revenue. The ability to quickly recover from cyberattacks is essential for maintaining operational resilience and ensuring the uninterrupted delivery of services. This need for continuity drives the development of comprehensive incident response plans and recovery strategies, providing that businesses can withstand and rebound from cyber incidents.

The legal and regulatory implications of cybersecurity are becoming increasingly pronounced. Governments worldwide enact laws and regulations to protect consumer data and ensure organizations implement adequate cybersecurity measures. Noncompliance with these regulations attracts hefty fines and signifies a failure in corporate responsibility, which can have lasting reputational consequences. These evolving legal frameworks underscore the need for organizations to stay abreast of legal requirements and embed compliance into their cybersecurity strategies.

Cybersecurity transcends technical and corporate realms, emerging as a social responsibility. In an interconnected world, the actions of one entity can have far-reaching impacts on others. Ensuring the security of digital systems is not just about protecting individual or corporate interests but also about safeguarding the broader community. It involves a commitment to ethical practices, a focus on education and awareness, and a collaborative approach to security, recognizing that we are all interconnected and responsible for each other's safety in the digital world. As we navigate the complexities of

cybersecurity, it is essential to remember that it is not just a technical issue but a critical component of our social fabric in the digital age.

THE PURPOSE OF THIS BOOK

Cybersecurity is as vast as it is vital, and navigating its waters can be as daunting as necessary. This book aims to serve as a compass in this journey, offering guidance and insight into the multifaceted world of cyber careers. Its purpose is fourfold: to introduce you to the diverse landscape of cybersecurity careers, to assist in preparing you for choosing a suitable career path, to shed light on the art of building professional networks, and to provide strategic advice on the hiring process in this dynamic field.

First, this book provides an introduction to the world of cyber careers. Cybersecurity is not a monolithic field but a tapestry of various specializations and roles, each addressing different aspects of digital security. From frontline defenders like security analysts to strategists and policymakers, this book explores the breadth of career paths available, detailing the skills, responsibilities, and challenges of each. This exploration is designed to give you a comprehensive view of the opportunities in cybersecurity, which will allow you to make informed decisions about where your interests and skills could be best applied.

Second, the book aims to help prepare you to choose a career in cybersecurity. Choosing a career is significantly influenced by personal interests, strengths, and market demand. We delve into the factors that should be considered when making this decision, including the evolving nature of cyber threats, the skill sets required for various roles, and the career trajectories that these roles offer. This guidance will equip you with the knowledge to align your career choice with personal aspirations and industry needs.

Building alliances through networking is another key focus of this book. In the ever-changing world of cybersecurity, professional networks can be a source of opportunities, learning, and support. We explore building and maintaining these networks, engaging with peers and mentors, and leveraging these relationships for mutual growth and learning. Effective networking strategies, both in-person and digital, are discussed, highlighting their role in career development and industry engagement.

This book offers insights into the cybersecurity hiring process. Securing a job in this competitive field requires more than just technical know-how; it demands an understanding of the hiring landscape, the ability to showcase your skills effectively, and the knowledge to navigate job interviews and assessments. From crafting a compelling resume to acing interviews and

understanding the expectations of employers in cybersecurity, this book provides practical advice and strategies to increase your chances of landing a job that aligns with your career aspirations in cybersecurity.

This book guides aspiring cybersecurity professionals, offering a comprehensive overview of the field, actionable advice on career selection and preparation, strategies for building effective professional networks, and practical tips for navigating the hiring process. Whether you are just starting to explore the field of cybersecurity or looking to make a more informed career choice, this book aims to be a valuable resource in your professional journey.

THIS BOOK IS A LIVING DOCUMENT

Like the cybersecurity field, this book is a living document. It is an evolving repository of knowledge and insights, shaped not only by the advancements in the field but also by the experiences and contributions of its readers. As you navigate through its chapters, you are encouraged to absorb and actively engage with the information.

First and foremost, I invite you to review the contents of this book and gain your own experiences. The theoretical knowledge provided here is a foundation, but the actual depth of understanding comes from applying these concepts in real-world scenarios. Whether through internships, projects, or professional roles, your experiences will add layers to your foundational knowledge and help you grow as a cybersecurity professional.

Your feedback is invaluable. I encourage you to connect with me on LinkedIn (https://www.linkedin.com/in/jasonedwardsdmist/) and share your thoughts, insights, and experiences. This feedback will help refine and update the book and contribute to the collective learning of the cybersecurity community. Your perspectives, challenges, and successes can enlighten and inspire revisions, making this book a more relevant and practical guide for others.

Paying it forward is a central theme of this book. Cybersecurity is not just about protecting networks and data; it is about building a knowledgeable, vigilant, and supportive community. I encourage you to help others learn about cyber careers and defend themselves in the digital world. Share your knowledge, mentor aspiring professionals, and contribute to forums and discussions. In doing so, you strengthen the entire community against evolving cyber threats.

Building your brand in the field of cybersecurity is also crucial. Your brand reflects your expertise, values, and contributions to the field. Engage with the community through social media, blogs, or speaking engagements. Share

your insights, discuss emerging trends, and showcase your achievements. A strong personal brand will open new doors and opportunities in your career.

Finally, remember that the time to start or advance your career in cybersecurity is today, not tomorrow. The field is rapidly growing, with opportunities emerging as quickly as the threats it contends with. Do not wait for the perfect moment; begin your journey now, armed with the knowledge from this book and a commitment to continuous learning and improvement. Your initiative today will shape your professional journey in the dynamic world of cybersecurity.

2

PATHS OF CYBERSECURITY EDUCATION

The journey into cybersecurity is anchored in a diverse array of essential skills and knowledge. These foundational elements are critical for anyone aspiring to make a mark in this field. Technical skills form the backbone of cybersecurity expertise. Networking and system administration proficiency are crucial because these skills provide the groundwork for understanding how systems communicate and function. This knowledge is essential for identifying vulnerabilities, securing networks, and managing systems effectively. A deep understanding of networking concepts, such as Transmission Control Protocol and Internet Protocol, firewalls, and network protocols, alongside practical system administration skills, equips individuals to tackle complex cybersecurity challenges.

In parallel with technical skills, soft skills play an equally vital role in cybersecurity. Critical thinking and effective communication stand out as key competencies. Analyzing situations, thinking logically, and solving problems are indispensable in a field where threats constantly evolve, and each new challenge requires a unique approach. Communication skills are equally important since cybersecurity professionals must explain complex technical issues to nontechnical stakeholders, write clear and concise reports, and work collaboratively with diverse teams.

Understanding the foundations of cybersecurity is another critical area of focus. This includes a thorough grasp of concepts like cryptography, which is fundamental for securing data, and risk management, which is essential for identifying, assessing, and mitigating cybersecurity risks. Knowledge of these areas ensures that cybersecurity professionals can develop strategies to protect against breaches and respond effectively to incidents.

Industry-specific knowledge can significantly enhance a cybersecurity professional's effectiveness. Different sectors, such as finance and healthcare, face unique cybersecurity challenges and regulatory requirements. Protecting financial transactions and complying with standards like the Payment Card Industry Data Security Standard are paramount in finance. In healthcare, securing patient data and adhering to the Health Insurance Portability and Accountability Act regulations are critical. A deep understanding of these industries' specific cybersecurity needs and challenges can make cybersecurity professionals more effective and sought-after in their fields.

UNIVERSITY PROGRAMS

University programs are essential in preparing the next generation of cybersecurity professionals. These programs, offered by leading institutions, blend academic rigor with practical experience, ensuring that graduates are well-equipped to tackle the challenges of the cybersecurity field.

The University of Texas at San Antonio (UTSA) is at the forefront of cybersecurity education and is renowned for its comprehensive approach to cyber-defense education. UTSA's curriculum covers a broad spectrum, from network security fundamentals to cyber operations and threat intelligence complexities. This broad coverage ensures that students are not only versed in current practices but are also prepared to adapt to emerging threats and technologies. UTSA's commitment to research and innovation further enriches the student experience by providing opportunities to engage in cutting-edge projects and to collaborate with leading experts in the field.

Hallmark University distinguishes itself with a curriculum that emphasizes practical skills. Their programs are meticulously crafted to balance theoretical knowledge with real-world application, focusing on making students job-ready. By integrating hands-on training and simulations, Hallmark ensures that graduates are knowledgeable and adept at applying their skills in various cybersecurity scenarios. This approach is invaluable in an industry where practical problem-solving abilities are as crucial as theoretical knowledge.

Georgetown University's cybersecurity program is noted for its holistic education, spanning technical skills, policy, and legal aspects of cybersecurity. This broad-based curriculum prepares students to understand and address cybersecurity challenges from multiple dimensions, a necessity in a field that intersects with various sectors and disciplines. Georgetown's emphasis on policy and legal aspects is particularly crucial, as it prepares students to navigate

the complex regulatory landscape and understand the broader implications of cybersecurity measures.

The U.S. Military Academy at West Point and the U.S. Air Force Academy offer unique programs that merge cybersecurity education with military discipline. These institutions focus on developing leaders skilled in cybersecurity and capable of making strategic decisions under pressure. The curriculum at these academies is rigorous, combining technical cybersecurity training with leadership and strategic studies. This comprehensive approach is designed to prepare graduates for critical roles in national defense, where they are tasked with protecting sensitive information and national infrastructure from cyber threats.

The curriculum in these university programs often includes specialized areas such as digital forensics, ethical hacking, cloud security, and cybersecurity management. This specialization allows students to delve deeply into specific areas of interest that will prepare them for niche roles in the cybersecurity ecosystem. These areas of specialization are constantly evolving, reflecting the dynamic nature of the field and the need for professionals who are specialists in their domains.

Internships and cooperative education opportunities are integral to these programs. They provide students with invaluable exposure to real-world scenarios, enhancing their learning and giving them a taste of the professional world. These experiences are crucial for building practical skills, understanding workplace dynamics, and developing professional networks. Internships often lead to full-time employment opportunities because employers value the hands-on experience that these programs provide.

After graduation, the avenues that are open to alums of these programs are diverse and abundant. Graduates find themselves well-positioned for roles across various sectors, including government agencies that play a vital role in national security; private sector companies, where they protect critical data and infrastructure; and nonprofit organizations that contribute to broader societal security. Many graduates pursue careers in consulting where, by leveraging their expertise across different industries or in academia and research, they contribute to advancing cybersecurity knowledge.

University programs in cybersecurity are crucial for developing a skilled and adaptable workforce that is capable of addressing the diverse and complex challenges of the cybersecurity landscape. These programs provide the foundational knowledge, specialized skills, and practical experience necessary for a successful career in this dynamic and critically important field (see Tables 2.1 and 2.2).

Table 2.1 Selected online cybersecurity degree colleges in the United States

Institution	Location	Program Highlights
Regent University	Virginia Beach, VA	BS in Cybersecurity Online; National Center of Academic Excellence in Cyber Defense
Maryville University of St. Louis	St. Louis, MO	BS in Cybersecurity Online Tracks in Offensive, Defensive, and General Cybersecurity
Indiana Wesleyan University–National & Global	Marion, IN	BS in Cybersecurity Online; Prepares for certification programs
Mississippi State University	Starkville, MS	BAS in Cybersecurity Online; Focuses on cyber systems and defense, ethical hacking
University of Illinois at Springfield	Springfield, IL	BS in Information Systems Security Online; National Center of Academic Excellence in Cyber Defense Education
University of Arizona	Tucson, AZ	BAS in Cyber Operations Online; Concentrations in Engineering, Defense & Forensics, Cyber Law & Policy
Franklin University	Columbus, OH	BS in Cyber Security Online; Center of Academic Excellence in Cyber Defense
Hallmark University	San Antonio, TX	BS in Cyber Security Online; MS in Cyber Security Online

Table 2.2 Selected (in-person) cybersecurity degree colleges in the United States

Institution	Location	Program Highlights
University of Maryland Global Campus	Adelphi, MD	Bachelor's and Master's in Cybersecurity, Software Development & Security, Digital Forensics & Cyber Investigation
American Public University System	Charles Town, WV	Bachelor's, Master's, and Certificate Programs in Cybersecurity
Western Governors University	Salt Lake City, UT	Cybersecurity Degrees with industry certifications
Davenport University	Grand Rapids, MI	In-person/Online Cybersecurity Education; National Center of Academic Excellence in Cyber Defense Education
Ferris State University	Big Rapids, MI	Associate, Bachelor's, Master's in Information & Security Intelligence
Drexel University	Philadelphia, PA	Bachelor of Science in Computing and Security Technology, Master of Science in Cybersecurity
DePaul University	Chicago, IL	Bachelor's and Master's in Cybersecurity; National Center of Academic Excellence in Cybersecurity
Rochester Institute of Technology	Rochester, NY	Bachelor's in Cybersecurity; Global Cybersecurity Institute
Community College of Allegheny County	Pittsburgh, PA	Associate in Cybersecurity, I.T. Support Specialist, Cybersecurity Support Specialist certificate
Champlain College	Burlington, VT	Bachelor's in Computer & Digital Forensics, Computer Networking & Cybersecurity

ADULT PROFESSIONAL PROGRAMS

Adult professional programs play a crucial role in the cybersecurity education landscape, especially for individuals seeking to enhance their skills or who wish to transition to a cybersecurity career later in life. These programs are designed to cater to the unique needs of working professionals, offering flexible learning options that include evening and online courses. This flexibility is vital for balancing their education with work and personal responsibilities.

Evening and online courses have become increasingly popular, providing an accessible pathway for continued education. These courses are designed to be flexible and convenient, allowing learners to engage with material at their own pace and on their own schedule. This learning mode is particularly beneficial for those who are managing full-time jobs or family commitments. Online courses often utilize interactive platforms that include video lectures, virtual labs, and discussion forums, creating an engaging and comprehensive learning experience that rivals traditional classroom settings.

One of the leading training programs in this sphere is ThriveDX.com. ThriveDX's Cyber Academy offers a comprehensive training solution that addresses the cybersecurity industry's talent shortage and diversity gap. It provides a dynamic learning platform with over 1,000 hours of hands-on training and 300 real-world simulations, aligned with the National Initiative for Cybersecurity Education/National Institute of Standards and Technology 800-181 framework. The program offers flexible learning options, including full-time and part-time tracks, and emphasizes hands-on learning with real-world applications through immersive exercises and simulations.

The training program is unique in its focus on reskilling high-potential talent from diverse backgrounds, offering industry-driven, government-grade cybersecurity training. It adheres to an accelerated learning methodology and a streamlined curriculum that teaches the specific skills necessary to excel in the cybersecurity industry, regardless of the learner's background.

ThriveDX has graduated over 50,000 students globally and maintains strong partnerships with over 50 universities and 500+ enterprise customers—earning recognition as a global leader in cybersecurity education. The program's duration varies, offering a full-time 12-week track or a part-time 24-week track to accommodate different learners' needs. Graduates are equipped for various roles in the cybersecurity industry, such as Cyber Defense Analyst and Cyber Incident Responder. No prior knowledge or background is required to participate, making the program accessible to individuals from diverse backgrounds, including those from nontechnical fields (see Table 2.3).

Table 2.3 ThriveDX Cybersecurity Bootcamp (online)

Course Title	Brief Description
Introductory Course	Entry-level exploration of networking, Linux and Windows operating systems, and virtualization concepts. Includes real-life cyberattack scenarios.
Microsoft Security	Focuses on managing networks and computers and setting up domain environments using Active Directory, DHCP, DNS servers, and other network services.
Computer Networking	Covers network devices, layers, and protocols, preparing students for the CompTIA Network+ certification exam.
Cloud Security	Involves understanding cloud storage and exploring platforms like Google Cloud, Microsoft Azure, and Amazon AWS. Prepares students for the AWS Certified Cloud Practitioner exam.
Linux Security	Teaches the Linux operating system, especially Kali Linux, and prepares students for the LPI Linux Essentials certification exam.
Network Security	Builds skills in managing, securing, and operating network communication equipment with preparation for the Cisco Certified CyberOps Associate exam.
Cyber Infrastructure & Technology	Explores various infrastructure defenses, secure architecture design, and working with SIEM solutions like Splunk.
Introduction to Python for Security	Provides instruction in basic programming with Python, setting up Python environments, and using tools for automating cybersecurity tasks.
Offensive Security: Ethical Hacking	Offers immersive exercises to understand cybercriminals, covering various cyberattacks and defense strategies.
DFIR & Threat Hunting	Focuses on advanced threat hunting methods, digital forensics, incident response, and the role of Security Operations Center teams.
Game Theory Strategy in Cybersecurity	Teaches innovative ways to solve defense issues by applying cyber tactics and game theory strategies to real-life cyberattacks.
Career Services	Dedicated to job search preparation in the cybersecurity industry, including interview training, networking, and resume writing.

Career transition pathways are a crucial focus of adult professional programs. For many professionals who are looking to shift into cybersecurity from different fields, these programs guide that transition. They often include career counseling, resume workshops, and interview preparation—all tailored toward the specific demands and expectations of the cybersecurity

job market. This holistic approach is invaluable for those looking to change careers, providing them with the necessary skills and guidance to navigate the job market.

When considering adult education options, one of the critical decisions is choosing between certificate programs and degree programs. Certificate programs typically focus on specific skills and are shorter in duration, making them a practical choice for those looking to gain specialized knowledge or update existing skills quickly. On the other hand, degree programs offer a more comprehensive education, covering a broad range of topics and often including opportunities for research and specialization. The choice between these options depends on individual career goals, time commitments, and the specific requirements of the roles they aspire to.

Balancing work, life, and education is a significant challenge for adult learners. Adult professional programs recognize this challenge and are structured to provide as much flexibility as possible. Time management is a crucial skill for students in these programs, as is the ability to prioritize and set realistic goals. Many programs offer resources to help students manage these challenges, including counseling services, time management workshops, and peer support groups. This support is essential in assisting adult learners to successfully navigate their educational journey without compromising their work or personal life.

In summary, adult professional programs offer a vital pathway for professionals seeking to enter or advance in cybersecurity. These programs provide the flexibility, support, and specialized training needed to succeed in this dynamic industry. Whether through evening and online courses, career transition support, or balancing education with other commitments, these programs are tailored to meet the diverse needs of adult learners, empowering them to achieve their career goals in cybersecurity.

SELF-STUDY PROGRAMS

Self-study programs in cybersecurity offer a flexible and personalized path for individuals who are eager to delve into the field at their own pace. These programs are particularly suited for those who seek autonomy in their learning process or for professionals looking to upskill alongside their current job commitments. The key to success in self-study lies in identifying and utilizing the wealth of online resources that are available.

One of the most prominent resources in the realm of self-study cybersecurity education is Cybrary. Cybrary has carved out a niche as a leading platform, offering an extensive range of cybersecurity courses. Cybrary provides learners with access to knowledge, from fundamental concepts to advanced topics. The platform is renowned for its user-friendly interface and the quality of its instructional content, which is both comprehensive and up-to-date. For those embarking on a self-study journey in cybersecurity, Cybrary stands as a beacon, guiding learners through the complexities of the field with its expertly crafted courses and resources.

Apart from Cybrary, other valuable online resources such as Coursera, Udemy, and MIT OpenCourseWare exist. These platforms host courses ranging from introductory to advanced levels, often designed and taught by experts in the field. They offer a mix of free and paid courses, providing learners with flexibility in terms of content and cost. These resources are ideal for creating a structured learning plan that caters to individual learning objectives and pacing.

Creating a structured learning plan is critical for practical self-study. This involves setting clear goals, choosing relevant courses, and allocating specific times for study. A well-structured plan helps to maintain focus and direction, ensuring that learning is consistent and comprehensive. It also involves balancing various topics, from technical skills like network security to theoretical knowledge like cybersecurity policies, to gain a holistic understanding of the field.

Staying motivated and accountable is another challenge in self-study programs. Without the external structure of a traditional classroom, self-learners need to cultivate discipline and motivation. Setting regular milestones, rewarding progress, and maintaining a dedicated study space can help sustain motivation. Additionally, keeping track of learning progress and continuously challenging oneself with practical projects or quizzes ensures that learning is compelling and engaging.

Joining online communities and forums is an excellent way to complement self-study programs. Communities such as Stack Overflow, Reddit's cybersecurity forums, and LinkedIn groups provide platforms for learners to ask questions, share knowledge, and stay updated with the latest industry trends. These communities also offer networking opportunities, allowing learners to connect with professionals and peers. Engaging in these communities can provide practical insights, peer support, and a source of motivation and inspiration.

Self-study programs in cybersecurity are a viable and effective means of acquiring knowledge and skills in the field. By leveraging resources like Cybrary, creating a structured learning plan, staying motivated, and engaging with online communities, learners can navigate the complexities of cybersecurity and build a solid foundation for their careers or further studies.

IMPORTANCE OF CONTINUOUS LEARNING

In the ever-changing cybersecurity landscape, continuous learning is not just beneficial—it is essential. The field is characterized by rapidly evolving technologies and methodologies, making it crucial for professionals to keep abreast of the latest developments. This ongoing learning process can take many forms, from formal education to self-directed study. Staying updated with technological advancements ensures that cybersecurity professionals can effectively defend against new and emerging threats. It also fosters innovation since understanding the latest trends can lead to developing novel security solutions.

Networking and professional development are critical components of continuous learning in cybersecurity. Engaging with peers, attending industry conferences, and participating in workshops and webinars offer valuable opportunities to exchange knowledge and experiences. These interactions provide insights into current best practices and open doors to potential collaborations and career advancements. Building a solid professional network can be a significant asset, offering support, advice, and access to opportunities that might not be available through formal channels.

The role of mentorship in cybersecurity education and career growth is substantial. Having a mentor offers numerous benefits, including guidance on career development, insights into industry trends, and advice on navigating professional challenges. Mentors can also provide practical support, such as helping with understanding complex concepts or offering feedback on projects. A mentor can be a guiding light for those new to the field, while experienced professionals can gain fresh perspectives and stay connected to the broader community (see Table 2.4).

Table 2.4 Finding a mentor checklist

Step Number	Step Description	Details
1	Identify your goals	Clearly define what you want to achieve in your professional career and what kind of guidance you seek.
2	Research potential mentors	Look for individuals with expertise in your area of interest. Utilize LinkedIn, professional organizations, and your network.
3	Evaluate compatibility	Consider the mentor's background, mentoring style, and availability to ensure a good match with your needs.
4	Prepare your request	Draft a clear, concise, and respectful message or email. Mention your goals, why you chose them, and what you hope to gain.
5	Reach out	Send your request. Be professional and polite. If using email, use a clear subject line like "Mentorship Inquiry."
6	Follow up	Send a polite follow-up if you don't hear back in a week or two. Respect their decision if they're unable to commit.
7	Discuss expectations	Once a mentor agrees, discuss expectations, goals, communication frequency, and methods.
8	Establish a mentorship agreement	Agree on a mentorship plan. This might include regular meetings, objectives, and feedback methods.
9	Engage actively and respectfully	Be proactive in the relationship. Prepare for meetings, be open to feedback, and respect their time.
10	Express gratitude and give feedback	Regularly thank your mentor for their guidance. Provide feedback about what's working and what could be improved.

The importance of continuous learning in cybersecurity cannot be overstated. Keeping up with evolving technologies, engaging in networking and professional development, seeking mentorship, and pursuing certifications and advanced training are all crucial for maintaining relevance and effectiveness in this dynamic field. This commitment to ongoing education ensures that cybersecurity professionals are well-equipped to protect against current and future cyber threats.