

THE CYBERSECURITY
WORKFORCE OF
TOMORROW

The Future of Work

The future of work is a vital contemporary area of debate both in business and management research and in wider social, political, and economic discourse. Globally relevant issues, including the aging workforce, rise of the gig economy, workplace automation, and changing forms of business ownership, are all regularly the subject of discussion in both academic research and the mainstream media, having wider professional and public policy implications.

The Future of Work series features books examining key issues or challenges in the modern workplace, synthesizing prior developments in critical thinking, alongside current practical challenges in order to interrogate possible future developments in the world of work.

Offering future research agendas and suggesting practical outcomes for today's and tomorrow's businesses and workforce, the books in this series present a powerful, challenging, and polemical analysis of a diverse range of subjects in their potential to address future challenges and possible new trajectories.

The series highlights what changes still need to be made to core areas of business practice and theory in order for them to be forward-facing, more representative, and able to fulfill the industrial challenges of the future.

OTHER TITLES IN THE SERIES

Careers: Thinking, Strategising and Prototyping
Ann M. Brewer

Algorithms, Blockchain and Cryptocurrency: Implications for the Future of the Workplace
Gavin Brown and Richard Whittle

HR Without People? Industrial Evolution in the Age of Automation, AI, and Machine Learning

Anthony R. Wheeler and Ronald M. Buckley

The Healthy Workforce: Enhancing Wellbeing and Productivity in the Workers of the Future

Stephen Bevan and Cary L. Cooper

Cooperatives at Work

George Cheney, Matt Noyes, Emi Do, Marcelo Vieta, Joseba Azkarraga and Charlie Michel

FORTHCOMING TITLES

Spending Without Thinking: The Future of Consumption

Richard Whittle

Inspiring Workplace Spirituality

Judi Neal

THE CYBERSECURITY WORKFORCE OF TOMORROW

BY

MICHAEL NIZICH

New York Institute of Technology, USA



United Kingdom – North America – Japan – India
Malaysia – China

Emerald Publishing Limited
Howard House, Wagon Lane, Bingley BD16 1WA, UK

First edition 2023

Copyright © 2023 Michael Nizich.
Published under exclusive licence by Emerald Publishing Limited.

Reprints and permissions service

Contact: permissions@emeraldinsight.com

No part of this book may be reproduced, stored in a retrieval system, transmitted in any form or by any means electronic, mechanical, photocopying, recording or otherwise without either the prior written permission of the publisher or a licence permitting restricted copying issued in the UK by The Copyright Licensing Agency and in the USA by The Copyright Clearance Center. Any opinions expressed in the chapters are those of the authors. Whilst Emerald makes every effort to ensure the quality and accuracy of its content, Emerald makes no representation implied or otherwise, as to the chapters' suitability and application and disclaims any warranties, express or implied, to their use.

British Library Cataloguing in Publication Data

A catalogue record for this book is available from the British Library

ISBN: 978-1-80382-918-0 (Print)

ISBN: 978-1-80382-915-9 (Online)

ISBN: 978-1-80382-917-3 (Epub)



ISOQAR

REGISTERED

Certificate Number 1985
ISO 14001

ISOQAR certified
Management System,
awarded to Emerald
for adherence to
Environmental
standard
ISO 14001:2004.



INVESTOR IN PEOPLE

To my wife Cara and to my children, Thomas and Grace. An achievement like this is neither accomplished nor celebrated alone. Without your love, support, and motivation throughout the writing process, none of this would have been possible. Thank you. I love you all very much.

CONTENTS

<i>List of Figures</i>	<i>xi</i>
<i>List of Tables</i>	<i>xiii</i>
<i>List of Abbreviations or Acronyms</i>	<i>xv</i>
<i>About the Author</i>	<i>xxv</i>
<i>Preface</i>	<i>xxvii</i>
<i>Acknowledgments</i>	<i>xxix</i>
1. An Introduction to the Field of Cybersecurity and the Current Workforce Gap	1
2. The Current and Future Technology of Cybersecurity	37
3. The Cyberhero and the Cybercriminal	63
4. Cybersecurity Products and Services	99
5. Preparing the Cybersecurity Workforce of Tomorrow	117
<i>Further Reading</i>	<i>147</i>
<i>Bibliography</i>	<i>159</i>
<i>Index</i>	<i>179</i>

LIST OF FIGURES

Chapter 1

Figure 1.	Sample Dark Web Network Architecture.	6
Figure 2.	ISC2 Cybersecurity Workforce Gap by Region.	16
Figure 3.	Five Pillars of the ITU Global Cybersecurity Index.	19
Figure 4.	NIST Risk Management Framework.	23
Figure 5.	Cybersecurity Maturity Model.	28

Chapter 2

Figure 6.	Sample Computer Network.	40
Figure 7.	Machine Learning Software Options.	43
Figure 8.	Blockchain Encryption Process.	47
Figure 9.	Sample Zero-Trust Architecture.	53
Figure 10.	Sample Chaos Monkey Workflow.	59

Chapter 3

Figure 11.	NICE Cybersecurity Workforce Framework.	68
------------	---	----

Chapter 5

- Figure 12. U.S. Department of Labor, Employment and Training Administration's Cybersecurity Competency Model. 122
- Figure 13. Knowledge Unit Usage Notional Structure. 125

LIST OF TABLES

Chapter 1

Table 1.	Types of Cybersecurity Attacks.	10
Table 2.	Types of Cyber Threat Actors.	11
Table 3.	The Five Pillars of the ITU Global Cybersecurity Index.	20
Table 4.	Key Risk Management Action Components.	22
Table 5.	Cyberspace Solarium Commission Report Proposals.	30

Chapter 2

Table 6.	Performance Attributes of 5G.	51
----------	-------------------------------	----

Chapter 3

Table 7.	NICE Cybersecurity Roles.	71
Table 8.	Recommendations to Aid in Retention.	89
Table 9.	Entry and Mid-Level Cybersecurity Jobs.	90

Chapter 4

Table 10.	Sample List of Kali Linux Tools.	105
-----------	----------------------------------	-----

Chapter 5

Table 11.	Work Role Category.	121
Table 12.	Professional Certificates in Cybersecurity.	128
Table 13.	Cybersecurity Competitions and Challenges.	136

LIST OF ABBREVIATIONS OR ACRONYMS

A&A	Assessment and Authorization
ADP	Automated Data Processing
AES	Advanced Encryption Standard
AFC4A	Air Force C4 Agency
AFI	Air Force Instruction
AFIWC	Air Force Information Warfare Center
AFOSI	Air Force Office of Special Investigation
AFPD	Air Force Policy Directive
AIMS	Automated Infrastructure Management System
AIS	Automated Information Systems
AMIDS	Audit Monitoring and Intrusion Detection System
ANSI	American National Standards Institute
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
ASD(C31)	Assistant Secretary of Defense for Command, Control, Communication and Intelligence
ASIMS	Automated Security Incident Measuring System
ASSIST	Automated System Security Incident Support Team
ATC	Authorization to Connect
ATD	Authorization Termination Date
ATM	Asynchronous Transfer Mode
ATO	Authorization to Operate
BIOS	Basic Input and Output System
BMA	Business Mission Area
C&A WG	Certification and Accreditation Working Group
C&A	Certification and Accreditation
C2	Command and Control
C2W	Command and Control Warfare

C4	Command, Control, Communications, and Computers
C4ISR	Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance
CA	Certification Authority
CAAP	Critical Asset Assurance Program
CAC	Common Access Card
CAL	Category Assurance List
CAP	Connection Approval Program
CC	Common Criteria
CCA	Clinger–Cohen Act
CCB	Configuration Control Board
CCI	Control Correlation Identifier
CD	Cross Domain
CDS	Cross-Domain Solution
CERT	Computer Emergency Response Team
CERT/CC	CERT/Coordination Center
CFR	Code of Federal Regulations
CI	Counterintelligence
CIAC	Computer Incident Advisory Capability
CIAO	Critical Infrastructure Assurance Office
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIPWG	Critical Infrastructure Protection Working Group
CIRT	Computer Incident Response Team
CISA	C4I Integration Support Activity
CITAC	Computer Investigation and Infrastructure Threat Assessment Center
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman, Joints Chiefs of Staff Instruction
CMDS	Computer Misuse Detection System
CMS	COMSEC Management System
CNA	Computer Network Attack
CNDSP	Computer Network Defense Service Provider
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COE	Common Operating Environment
COMSEC	Communications Security
CONOPS	Concept of Operations

COTS	Commercial Off-the-Shelf
CSA	Computer Security Act
CSIR	Computer (and Network) Security Incident Response
CSS	Central Security Service
CSSO	Computer Systems Security Officers
CUI	Controlled Unclassified Information
DAA	Designated Approving Authority (DAA)
DARPA	Defense Advanced Research Projects Agency
DASD	Deputy Assistant Secretary of Defense
DASD(DT&E)	Deputy Assistant Secretary of Defense for Developmental Test & Eval
DATO	Denial of Authorization To Operate
DCI	Director of Central Intelligence
DCID	Director of Central Intelligence Directive
DCMO	Deputy Chief Management Office
DCPDS	Defense Civilian Personnel Data System
DES	Digital Encryption Standard
DIA	Defense Intelligence Agency
DIACAP	DoD Information Assurance Certification and Accreditation Process
DIACCS	Defense IA Command and Control System
DIAMOND	Defense Intrusion Analysis & Monitoring Desk
DIAP	Defense Information Assurance Program
DIB	Defense Industrial Base
DIDS	Distributed Intrusions Detection System
DII	Defense Information Infrastructure
DIMA	DoD Portion of the Intelligence Mission Area
DIRNSA	Director, National Security Agency
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DITPR	DoD Information Technology Portfolio Repository
DITSCAP	DoD IT Security Certification and Accreditation Process
DITSWG	Defense Information Technology Security Working Group
DMC	Defense MegaCenter
DMS	Defense Message System
DNI	Director of National Intelligence
DNS	Domain Name Servers
DoD CIO	DoD Chief Information Officer
DoD ISRMC	DoD Information Security Risk Management Committee

DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	DoD Instruction
DoDIIS	DoD Intelligence Information System
DODIN	Department of Defense Information Networks
DoDM	DoD Manual
DoE	Department of Energy
DoN	Department of the Navy
DOT&E	Director, Operational Test and Evaluation
DREN	Defense Research and Engineering Network
DSAWG	Defense IA Security Accreditation Working Group
DSS	Defense Security Service
DT&E	Developmental Test and Evaluation
DTM	Directive-Type Memorandum
E/APL	Evaluated Approved Product
EAL	Evaluation Assurance Level
EFOIA	Electronic Freedom of Information Act
EIEMA	Enterprise Information Environment Mission Area
EITDR	Enterprise Information Technology Database Repository
eMASS	Enterprise Mission Assurance Support Service
EOP	Executive Office of the President
ETA	Education, Training and Awareness
ETAPWG	Education, Training, Awareness and Profes- sionalization Working Group
FIPSPUB	Federal Information Processing Standard Publication
FIRST	Forum of Incident Response and Security Teams
FISMA	Federal Information Security Management Act
FIWC	Fleet information Warfare Center
FN	Foreign National
FOIA	Freedom of information Act
FSO	Field Security Office
FTS	Federal Telecommunications Service
GAO	General Accounting Office
GCCS	Global Command and Control System
GCSS	Global Combat Support System
GIG	Global Information Grid
GMITS	Guidelines for the Management of IT Security
GOSC	Global Operations and Security Center
GOTS	Government Off-the-Shelf
GSA	General Services Administration

GSII	Government Services Information Infrastructure
HBSS	Host Based Security System
I&W	Indications and Warning
IA	Information Assurance
IAD	Information Assurance Document
IAG	Information Assurance Group
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IAPWG	Information Assurance Policy Working Group
IASE	Information Assurance Support Environment
IATAC	Information Assurance Technology Analysis Center
IATC	Interim Authority to Connect
IATO	Interim Authority to Operate
IATT	Interim Authority to Test
IAVA	Information Assurance Vulnerability Alert
IC	Intelligence Community
IEEE	Institute for Electrical and Electronics Engineers
INFOCONs	Information Operations Conditions
INFOSEC	Information Systems Security
INFOSYS	Information Systems
IO	Information Operations
IP	Internet Protocol
IPMO	INFOSEC Program Management Office
IPR	Internet Protocol Router
IPSec	Internet Protocol Security
IPTF	Infrastructure Protection Task Force
IRC	INFOSEC Research Council
IRM	Information Resource Management
IRS	Incident Reporting Structure
IRT	Incident Response Team
IS	Information System
ISO	International Organization for Standardization
ISRMC	Information Security Risk Management Committee
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
ITMRA	Information Technology Management Reform Act
IW	Information Warfare
IW-D	Information Warfare – Defensive
JCCC	Joint Communications Control Center

JCIDS	Joint Capabilities Integration and Development System
JDIICS	Joint DII Control Systems
JID	Joint Intrusion Detection
JIE	Joint Information Environment
JIEO	Joint Interoperability Engineering Organization
JIWG	Joint IA Operations Working Group
JPO STC	Joint Program Office for Special Technical Countermeasures
JTF-CNO	Joint Task Force – Computer Network Operations
JWICS	Joint Worldwide Intelligence Communications System
JWID	Joint Warrior Interoperability Demonstration
KMI	Key Management Infrastructure
KS	Knowledge Service
LE	Law Enforcement
LE/CI	Law Enforcement and Counterintelligence
LEA	Law Enforcement Agency
MA	Mission Area
MCDES	Malicious Code Detection and Eradication System
MLS WG	Multilevel Security Working Group
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NA	Not Applicable
NACIC	National Counterintelligence Center
NC	Non-Compliant
NCIS	Naval Criminal Investigative Service
NCSC	National Computer Security Center
NDU	National Defense University
NIAC	National Infrastructure Assurance Council
NID	Network Intrusion Detector
NII	National Information Infrastructure
NIPC	National Infrastructure Protection Center
NIPRNet	Non-Classified Internet Protocol Router Network
NISP	National Industrial Security Program
NIST	National Institute of Standards and Technology
NITB	National INFOSEC Technical baseline
NOC	Network Operating Centers
NOSC	Network Operation Security Center

NS/EP	National Security and Emergency Preparedness
NSA	National Security Agency
NSD	National Security Directive
NSIRC	National Security Incident Response Center
NSOC	National Security Operations Center
NSS	National Security System
NSTAC	National Security Telecommunications Advisory Committee
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NSU	Non-Standard Usage
OASD(C3I)	Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
OIG DoD	Office of the Inspector General of the Department of Defense
OMB	Office of Management and Budget
OPSEC	Operations Security
ORNL	Oak Ridge National Laboratory
OSD	Office of the Secretary of Defense
OSD/JS	Office of the Secretary of Defense/Joint Staff
OT&E	Operational Test and Evaluation
OUSD(P)	Office of the Under Secretary of Defense (Policy)
PAO	Principal Authorizing Official
PCCIP	President's Commission on Critical Infrastructure Protection
PGP	Pretty Good Privacy
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIT	Platform Information Technology
PKI	Public Key Infrastructure
PM	Program Manager
PM/SM	Program Manager/System Manager
POA&M	Plan of Action and Milestones
POM	Program Objective Memorandum
PPP	Program Protection Plan
PPS	Internet Protocol Suite and Associated Ports
PPSM	Ports, Protocols, and Services Management
PPTP	Point-to-Point Tunneling Protocol

RCERTs	Regional Computer Emergency Response Teams
RDT&E	Research, Development, Test and Evaluation
RMF	Risk Management Framework
ROSC	Regional Operations and Security Center
RT&E	Research, Test, and Evaluation
SABI WG	Secret and Below Interoperability Working Group
SABI	Secret and Below Interoperability
SAP	Special Access Program
SAPCO	SAP Central Office
SAR	Security Assessment Report
SATAN	Systems Administrators' Tool for Assessing Networks
SBU	Sensitive-But-Unclassified
SCA	Security Control Assessor
SCAO	SIPRNET Connection Approval Office
SCAP	Security Content Automation Protocol
SCCVI	Secure Configuration Compliance Validation Initiative
SCG	Security Configuration Guide
SCI	Sensitive Compartmented Information
SCRI	Secure Compliance Remediation Initiative
SECDEF	Secretary of Defense
SEI	Software Engineering Institute
SET	Secure Encrypted Transaction
SIO	Special Information Operations
SIPRNet	Secret Internet Protocol Router Network
SISO	Senior Information Security Officer
SITR	Secret Internet Protocol Router Network Information Technology Registry
SLA	Service-Level Agreement
SM	System Manager
SNAP	Systems/Networks Approval Process
SP	Special Publication
SPB	Security Policy Board
SRG	Security Requirements Guide
SSAA	Systems Security Authorization Agreement
SSE	System Security Engineering
STIGs	Security Technical Implementation Guides
T&E	Test and Evaluation
TAG	Technical Advisory Group
THREATCON	Threat Condition
TPM	Trusted Platform Module

TRANSEC	Transmission Security
TRMC	Test Resource Management Center
TSN	Trusted Systems and Networks
U.S.C.	United States Code
UC	Unified Capabilities
UCAO	Unclassified Connection Approval Office
UCDMO	Unified Cross Domain Management Office
UCMJ	Uniform Code of Military Justice
UR	User Representative
URL	Uniform Resource Locator (Universal Resource Locator)
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USD(P)	Under Secretary of Defense for Policy
USSTRATCOM	United States Strategic Command
VAAP	Vulnerability and Assessment Program
VAS	Vulnerability Assessment System
VPN	Virtual Private Network
WMA	Warfighting Mission Area

ABOUT THE AUTHOR



Dr. Michael Nizich, PhD, CISSP, is the Director of the Entrepreneurship and Technology Innovation Center (ETIC) and an Adjunct Associate Professor of Computer Science and Cybersecurity at New York Institute of Technology. He has more than 20 years of professional industrial leadership experience in Information Technology and Cybersecurity in a variety of industries, including aviation, education, law enforcement, and biotechnology. Nizich has held IT and Security leadership positions in both private and publicly held companies, higher education institutions, and nonprofit organizations.

He has more than 15 years of college-level teaching experience at four different colleges and universities and holds a PhD in Information Science from Long Island University, a master's degree in Technology Systems Management from Stony Brook University, and a bachelor's degree in Computer Information Systems from Dowling College. Nizich also holds a Certified Information Systems Security Professional (CISSP) certificate from the International Information System Security Certification Consortium (ISC²).

He additionally directs New York Tech's Center of Academic Excellence for Cybersecurity Education, designated by the U.S. Department of Homeland Security and the National Security Agency, is the recipient and principal investigator of several Department of Defense Cybersecurity grants, awardee of two NASA contracts for cybersecurity technologies, and has been interviewed and quoted in over 20 technology-related articles in leading publications including the *Communications of the ACM*, *CIO Review*, *Crain's New York*, *The Economist*, and *InfoSecurity Magazine* representing over 5 million readers. Dr. Nizich is a leader in the field of Information Technology and Cybersecurity, the Chair of the NY Metro ACM Chapter, Education Committee Chair and board member of ISC² Long Island, and serves on various industrial and institutional advisory boards in a technology role.

PREFACE

Cybersecurity continues to be one of the fastest growing and expanding fields and is yet again forecasted for near exponential growth in new hires, corporate and government investment, and corporate and government losses from preventable breaches. Yet, we still do not have a comprehensive and synergetic understanding of the cybersecurity ecosystem between industry and government security leaders, the cybersecurity workforce, the emerging cybersecurity workforce, educational institutions, and the human resources sector which still struggles with recruitment and retention of new cybersecurity talent.

It is for this reason that I decided to research and write this book. The purpose was to provide a single point of reference that would provide a variety of readers with an understanding of the current field of cybersecurity, the most probable future of the field based on current trends and an illustrative guide to understanding the relationships and interdependencies of the various components that make up the field. These components include the various technologies that make up cybersecurity, emerging technologies, current cybersecurity workforce, emerging cybersecurity workforce, educational institutions, and of course the organizations that require the security in the first place. Additionally, the criminal element and the driving

forces of cybercrime are included in these components since they are the impetus for the entire movement.

This book incorporates several different approaches in its scaffolding that I felt worked well to bring everything together for the reader. The overall approach was to first perform and implement a literature review of over 100 articles, books, websites, and interviews from industry, government, and educational leaders in the field. Next was to include a series of expert opinions and scenario-based thought experiments in each chapter to help the reader to position themselves in one of the scenario roles and hear from experts in the field. I then include probabilistic descriptions of the future of cybersecurity based on the topics discussed in the chapter coupled with the current and forecasted trends. And finally, I included a library of resources for the reader, regardless of their roles, to quickly access during their cybersecurity journeys for whatever challenges they may encounter and at any level.

In summary, this book is not intended to make the reader a cybersecurity expert but is intended to provide the reader with a broad understanding of how the various components of the cybersecurity field work together, explain current trends that are occurring, and provide insights as to what the probabilistic future of cybersecurity and the workforce will be so the readers can get better prepared for the future, regardless of what their specific role in cybersecurity is now, or will be in the future.

ACKNOWLEDGMENTS

I would like to acknowledge the researchers and authors whose prior research and writing made this work possible, thank you all for allowing me to stand on the shoulders of giants. A special thank you to all of the cybersecurity experts in industry, academia, and government who were so accommodating during my research and finally, a special thank you to all at Emerald Publishing who believed in this work and the value that it will provide to individuals and organizations in government, industry, and academia as they help to build the cybersecurity workforce of tomorrow.