THE FUTURE OF WORK

THE CYBERSECURITY WORKFORCE OF TOMORROW

Michael Nizich

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

emerald PUBLISHING

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

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

First edition 2023

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

Certificate Number 1985
ISO 14001

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

LIST OF FIGURES

Chapter 5

LIST OF TABLES

Chapter 5

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 Professionalization 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 (ISC^2).

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 ISC^2 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.

This page intentionally left blank

1

AN INTRODUCTION TO THE FIELD OF CYBERSECURITY AND THE CURRENT WORKFORCE GAP

INTRODUCTION

Throughout this book, there are numerous topics discussed in the area of cybersecurity including breaches, technology, data loss and prevention, and the cybersecurity workforce gap to name a few. However, to adequately place them in context to the future of cybersecurity as a field, as an industry, and most relevantly, with regards to the cybersecurity workforce of tomorrow, a brief but detailed look at the background and history of cybersecurity is imperative to fully grasp the relationships between the various components that comprise cybersecurity.

So what is cybersecurity? Cybersecurity can be defined as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets" (ITU, 2008) or as "both about the insecurity created through cyberspace and about technical/non-technical practices of making it (more) secure" Dunn-Cavelty (2010). There are several different ways to look at cybersecurity and

they are from the perspective of both protective measures and of threats to data and systems. Protective measures focus on the mechanisms that defend against unauthorized use, modification, or exploitation, while threats to data and systems focus on the determinants of a system breach and the consequences of a breach such as organizational losses.

Cyberattacks are commonly known to adversely affect the functionality of computer systems (Nye, 2018) and can be thought of as any outside attack that could compromise the security of an organization or a system inside the organization (Sharma, Gandhi, Mahoney, Sousan, & Zhu, 2010). Malicious cyberattacks are acts that are carried out with the intent of destroying data or documentation for the users (Wood, 2000) and cybersecurity threats can hugely impact organizations, assets, and the people involved (Von Solms & Van Niekerk, 2013).

There are a few different perspectives that can be taken when considering the cybersecurity workforce of tomorrow. These primarily include the cybersecurity student, the job seeker, the transitional worker, the advancing cybersecurity professional and the human resource professional. Each perspective has its own interests and concerns regarding the future of the cybersecurity workforce including, respectively, what do I need to learn to become a cybersecurity professional? How do I find a job in cybersecurity now and in the future? How do I prepare for the future and continue to advance my cyber career? And how do I continue to competitively attract, recruit, and retain cybersecurity professionals at my corporate, government, or nonprofit organization?

Unfortunately, there is one more perspective to be considered when discussing the cybersecurity workforce of tomorrow and that is from the perspective of the cybercriminal. If the methods and behaviors of cybercriminals are not considered, the edge will be lost in understanding what we need to do to prepare for the future since we will not know

what mischief the criminal element is preparing for us. The criminal element, now in a very organized fashion, researches, tests, and prepares malicious attacks that compromise our valuable data, and their methods will become more advanced with the introduction of more advanced technologies. As cyber professionals use these advancements to protect systems, cybercriminals are using these advances to come up with new ways to bypass any obstacles implemented by those professionals responsible for protecting the systems.

THE COST OF CYBER CRIME

Billions of dollars are spent on Cybersecurity each year on a global scale (Koch, 2017). In 2015, it was predicted that about $75 billion had been used to fight cybercrime and that the global cybersecurity market is expected to expand to $170 billion by 2020 (Morgan, 2015) which has now surpassed even that estimate. According to the Ponemon Institute's 2019 Cost of a Data Breach Study (Ponemon, 2019), the average cost of a data breach in 2019 is $3.92 million (Koch, 2017), or stated otherwise, $150 per lost or stolen record, a 1.6% increase from 2018.

Cybercrime and more specifically successful cyberattacks can cause devastating financial losses and negatively affect organizations and individuals as well. It's estimated that a data breach costs 8.19 million USD for the United States and 3.9 million USD on an average (IBM security report), and the annual cost to the global economy from cybercrime is 400 billion USD (Fischer, 2014). According to Juniper Research (Juniper Research, 2019), the number of records breached each year to nearly triple over the next five years. Thus, it's essential that organizations need to adopt and implement a

strong cybersecurity approach to mitigate the loss. The national security of a country depends on the business, government, and individual citizens having access to applications and tools which are highly secure, and the capability of detecting and eliminating such cyber threats in a timely way. Therefore, to effectively identify various cyber incidents either previously seen or unseen, and intelligently protect the relevant systems from such cyberattacks, maintaining a highly skilled cybersecurity workforce is essential.

Several high-profile data breaches have occurred in recent years including the well-known breaches at companies like Facebook, Equifax, Exactis, and Under Armour. These incidents have renewed concerns about cybersecurity. In July 2017, Equifax's data breach affected over 143 million individuals, compromising such personal information as social security numbers, credit cards, drivers' licenses, dates of birth, phone numbers, and email addresses (Fleishman, 2018). Facebook's 2019 data breach similarly impacted 540 million records of individuals' personal information (Silverstein, 2019). Information from 340 businesses and individuals were affected by marketing firm Exactis' breach in June 2018 (Greenberg, 2018). The retail industry is not exempt, with Under Armour's May 2018 breach exposing 150 million customers' information. It is no longer a question of whether a data breach will occur, but rather when (Cheng & Walton, 2019), and understanding the attributes and contributing factors to maintaining a strong and effective cybersecurity workforce both now and in the future is imperative to the safety and well-being of all countries and people on a global level.

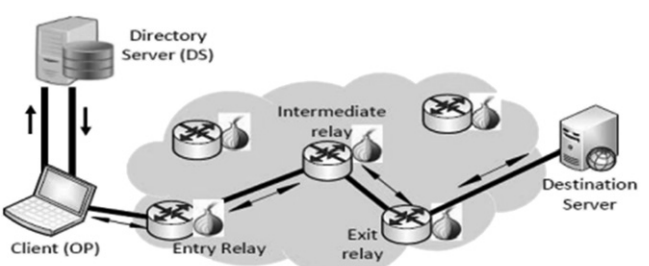
THE MARKET FOR STOLEN DATA

It is important to discuss an important driving force for the increase in both frequency and complexity of cyberattacks and that is the marketplace for stolen data. With any crime, specifically theft, there needs to be someone, commonly known in criminal justice, as a fence to sell the stolen goods to. In noncybercrimes, this is why we see burglars that only steal certain things from houses because they have someone that they know will buy it, buy it quickly and for a fair price. This is also why criminals develop modus operandis or MOs (methods of operation) which help us to identify them during our investigations. Similarly in the cyber world, criminals steal very specific data and their fences, instead of hanging out in a seedy bar in a dimly lit part of town, are hanging out on the dark web. The dark web is a network of specifically designed and generally untraceable websites and communications infrastructures for criminals to buy and sell stolen data. It is very difficult to, from a law enforcement perspective, locate, identify, and build solid cases against suspects operating on the dark web. It is even more difficult to prosecute criminals and to receive a guilty verdict from a jury of peers based on the sometimes broad and nonspecific body of evidence that can be acquired from system access logs and data retrieved from a home arrest based on a warrant.

Think of the dark web as the local shopping mall with stores and kiosks or the famous Marrakech markets, but instead of scarves and blue jeans, they are selling data, lots and lots of data. The dark web is the hidden collective of internet sites only accessible by a specialized web browser. It is used for keeping internet activity anonymous and private, which can be helpful in both legal and illegal applications. While some use it to evade government censorship, it has also been known to be utilized for highly illegal activity

(Kaspersky, 2022). However, the dark web comprises only a small portion of the entire internet while the rest comprises what is called the open web and the deep web. The open web is what we consider as visible to the public and makes up a very small percentage of web content. The deep web sits below the surface and accounts for approximately 90% of all websites. This portion of the web consists of things like company files, organizational databases, and internal intranets. An essential component of the dark web is browsers. Websites are hosted in an overlay network technology in the dark web, which is not accessible without special-purpose browsers like Tor (The Onion Router) or I2P (Invisible Internet Project) (Saleem et al., 2022). An example of a dark web network architecture can be seen in Fig. 1.

The dark web refers to sites that are not indexed and only accessible via specialized web browsers. The dark web, however, is a very concealed portion of the deep web that few will ever interact with or even see. One way to look at it is that the deep web covers everything under the surface that's still accessible with the right software, including the dark web, and this makes the dark web very attractive to criminals in that there is no webpage indexing by surface web search engines,



Source: Original diagram using Visio to create.

Fig. 1. Sample Dark Web Network Architecture.

there are virtual traffic tunnels that are only inaccessible by traditional browsers like Chrome or Firefox, and finally, it's further hidden by various network security measures like firewalls and encryption.

For the cybersecurity workforce of the future, professionals will need to be far more familiar with the workings of the dark web than they are required to be today. This not only includes a knowledge of the technical aspects of the dark web but also a willingness to work with law enforcement at city, state, and federal levels as there will be an increased push to identify and penalize cybersecurity offenders. As seen in the Solarium report, there is now a proposed structure to increase and intensify the law enforcement side of cybersecurity prosecution which means that cyber professionals will need to become more adept at identifying the details of the cybercrime from a criminal case perspective and not just a deterrence and recovery perspective. Currently, cyber professionals focus on working hard to deter any kind of attack and, if attacked, recovering quickly, efficiently, and affordably from that attack. Very few cybersecurity professionals today are focused on identifying the criminal, prosecuting the criminal, and stopping them from committing future cybercrimes.

CYBERATTACK METHODS

The modern computer network transfers data from one computer to another using a standardized process or protocol called the TCP/IP (Transmission Control Protocol/Internet Protocol) model. This process involves the deconstruction and reconstruction of information from simple binary values (0 or 1) that are represented as electrical signals over copper cables and Radio Frequency (RF) networks. These signals are

then reconstructed into complex data representations that can be opened and accessed by advanced programs like Microsoft Word, Outlook, and so forth. Any cyberattack that manipulates these data between users in any of its states, such as a man-in-the-middle attack, or denies the ability of any one computer to contact any other computer, such as a denial of service attack, causes the network and its functional components such as switches, routers, and firewalls to operate as if they are at full capacity while they are really being underutilized at that time. In other words, the network breaks.

Like any common criminal, a cyberattacker has an MO in which they have a very specific crime that they commit and a very specific way in which they commit that crime. These MOs are usually geared around their ultimate criminal goal and their purpose for the attack. Some criminals are looking to profit financially from their exploits while others are seeking a change or alter some sort of political outcome. Whatever the reasoning is for the attack, these activities can all be considered malicious cyberattacks.

So what is a malicious cyberattack? A malicious cyberattack, if successful, allows unwanted access to unauthorized actors, resulting in potential loss of information integrity (Boyes, 2015). There are also nonmalicious acts that threaten the confidentiality, integrity, and availability of information within a system. For instance, if access is mistakenly granted to an unauthorized employee outside a project team, any intentional or unintentional change in the data leading to serious implications is counted as a cyber breach (Sommer & Brown, 2011). There are different forms of cyberattacks which might cause damage or disrupt the assets (Peng, Lu, Liu, Gao, Guo, & Xie, 2013). The different threats include intellectual property theft, degradation of assets, malware, viruses, worms, and spyware. It is critical to protect information security assets, both physical and virtual, against malicious