Women in Engineering and Science

Debra A. Christofferson *Editor*

Women in Security

Changing the Face of Technology and Innovation

Springer

Women in Engineering and Science

Series Editor
Jill S. Tietjen
Greenwood Village, Colorado, USA

More information about this series at http://www.springer.com/series/15424

Debra A. Christofferson
Editor

Women in Security

Changing the Face of Technology and Innovation

Springer

Editor
Debra A. Christofferson
Tempe, AZ, USA

ISSN 2509-6427 ISSN 2509-6435 (electronic)
Women in Engineering and Science
ISBN 978-3-319-57794-4 ISBN 978-3-319-57795-1 (eBook)
https://doi.org/10.1007/978-3-319-57795-1

Library of Congress Control Number: 2017942744

Printed on acid-free paper

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

Foreword

Our personal and professional worlds are increasingly digital, and the information we share in this digital economy is proliferated across a multitude of networks. These networks have become so ubiquitous that we often engage with them without deliberate thought as to the information we provide. Whether playing online games, building our social network, conducting financial transactions, or shopping online, each time we engage with a network we provide another block of information. Each block of information on its own may seem innocuous; however, hackers have built a prosperous business by obtaining and consolidating disparate blocks of data into sensitive, saleable information.

While the risks with our personal information are immense, the risks to businesses are astronomical. In addition to maintaining legal compliance, ensuring the security of the business network is central to safeguarding a company's intellectual property, reputation, and relationships with its customers and suppliers. This is particularly germane in supply chain as suppliers are often the gateway into large organization networks. We've all heard countless examples of security breaches that originated in the supply chain, including the breach of Target's network which resulted in the theft of 40 million credit card numbers. Then there was the theft of 21.5 million records with highly sensitive personal information from the U.S. Government's Office of Personnel Management, and the pre-installation of a malicious app to steal passwords and credit card information on Android devices. In each of these cases, the hackers gained access through a supplier's network. Cyber breaches, such as these, have caused significant financial harm to businesses, from disrupting operations to extortion to industrial espionage. The reputational damage can be so severe that many businesses do not report breaches.

Without a doubt, such breaches have a drastic effect on consumers and businesses—with both short and long term effects. As society's dependence upon digitization increases so does the importance of cybersecurity. We're moving into a space of autonomous vehicles, increased internetworking of devices through adoption of the Internet of Things (IoT), wearables, and blockchain for records management and payment—all of which rely on sharing information across copious networks. The migration to cloud services, integration of suppliers, and implementation of

applications to analyze big data have resulted in the centralization of data. This is a huge target for hackers as it provides unparalleled access to massive amounts of data with just one attack. Thus, the protection of our networks is crucial.

We are reaching a tipping point. With the increased interconnectivity and consolidation of vast amounts of data, we're likely to experience an increase in cyber breaches. At the same time, we have a global shortage of professionals entering the cybersecurity field. The 2015 (ISC)2 Global Information Security Workforce Study[1] projected a shortfall of 1.5 million workers in cybersecurity by 2019. The study also showed that women comprised a **mere 10%** of the cybersecurity workforce globally.[2] Diversity is key to innovation, thus attracting women to this field is vital. In addition to diverse thought, women bring an inherent ability to collaborate, multitask, empathize, and take a holistic approach to problem solving. Since data is spread across multiple nodes and affects a wide range of people, protecting networks often requires bringing many organizations together to employ a holistic solution and secure our data. We need the skills that women bring if we are going to successfully address cybersecurity risks.

The scarcity of role models and mentors is one of the key obstacles in attracting women to this field. Several organizations have worked tirelessly to increase awareness of this field and attract and advance women in cybersecurity. This book is a milestone. The women are accomplished, talented, fierce, and, above all, excellent role models. The background of these innovative women in cybersecurity and their depth of knowledge will inspire other women. I encourage you to read this book, be inspired, and take action to address this important topic.

M.L. Peck

[1] The 2015 (ISC)2 Global Information Security Workforce Study, Frost & Sullivan, April 16, 2015, https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)2-Global-Information-Security-Workforce-Study-2015.pdf

[2] *Women in Security: Wisely Positioned for the Future of InfoSec*, Frost & Sullivan, 2015, https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/2015-Women-In-Security-Study.pdf

Contents

About the Editors

Juanita Agard was born in New York City, NY, and raised in the Seattle, Washington, area. She moved to the nation's capital to attend Howard University and pursued a bachelor's degree in System and Computer Science with a minor in Mathematics. Immediately after graduating, Juanita had an IT Specialist position with IBM waiting for her, and the experience confirmed her passion for entrepreneurship, Information Technology (IT), and technology law.

As cybersecurity emerged, it eventually developed its own career path, along with educational institutes creating cybersecurity curriculums. Juanita envisioned uniting her IT engineering experience with technology law to become a cybersecurity subject matter expert. She researched cyber education partnerships between companies and universities and job opportunities with companies offering cyber training.

Juanita landed a Software Requirement Engineer position with Booz Allen Hamilton, a company with a reputation for investing in their employees. Through the Booz Allen Cyber cohort program, Juanita immediately enrolled into the Cybersecurity Technology master program at UMUC and expects to complete it in 2017.

Ms. Agard has been with Booz Allen Hamilton for almost 4 years, majoring in a cybersecurity master's degree program at UMUC. She also obtained an **active security clearance** and is gaining all the cybersecurity experience she can.

In parallel, Agard too took the CompTIA Security +, and EC-Council Certified Ethical Hacker (CEH) boot camp trainings to obtain her cyber certifications. She is **studying for the CISSP** and planning to complete it this year. Ms. Agard also obtained a Cybersecurity Technology Graduate Certificate and has only two classes left to complete her master's in cybersecurity.

She currently is working at NASA as a cybersecurity policy analyst. Juanita is relatively new to the project and still on the learning curve as to how things operate. Her responsibilities are to capture the existing security change management process from

multiple projects, to develop a high-level Change Control Board charter. The overall goal is to have an overarching mechanism to manage IT security services agencywide.

On a previous project, she served as a Security Requirement Analyst, analyzing and consolidating NIST SP 800–53 security controls to import into a central repository for reusable and repeatable purposes for the FDA project.

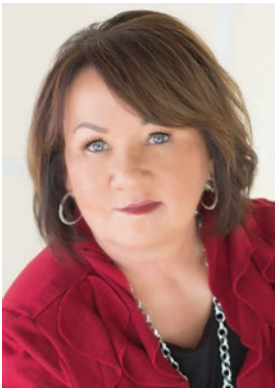
Diane Barrett holds a PhD in business administration with an information security specialization from Northcentral University. She is a Certified Information Systems Security Professional (CISSP) holding many additional industry certifications. Diane has an extensive background and has been involved in the IT industry for over 20 years. She is the President of NextGard technology, LLC and has done contract forensic and security assessment work for numerous years and held positions such as manager of research and training for Kroll's cyber division and forensic training director for Paraben Corporation.

Diane is the conference program chair for the Conference on Digital Forensics, Security and Law as well as the President of the Digital Forensics Certification Board. She has been involved in collegiate-level forensic education at Bloomsburg University, American Military University, and the University of Advancing Technology. She has co-authored several security and computer forensics books including *Security + Exam Cram, Virtualization and Forensics, and Cybercrime and Cloud Forensics: Applications for Investigation Processes*.

Lacey Chong is a national security consultant who specializes in business process improvement. She has over 13 years of experience working for the U.S. Department of Defense, U.S. Department of State, and several national-level intelligence agencies as a government civilian and as a consultant. Throughout her career, she has held various roles involving cybersecurity, project management, all-source intelligence analysis, and business process improvement. Most notably, she served as a Special Assistant at the National Security Council's Counterterrorism Policy Directorate from 2008 to 2011. Ms. Chong is currently an Associate with Booz Allen Hamilton in McLean, VA.

Ms. Chong holds a B.A. in Asian Studies from the University of Puget Sound, an M.A. in International Affairs/International Security from George Washington University, and a graduate certificate in Change Management from the Georgetown University Executive M.B.A. program. She founded Spa Swag for Warriors, a nonprofit charitable organization in 2015, and is currently a member of the Board's

Executive Committee. Selected as a 2016 Northern Virginian of the Year for her work with Spa Swag, she directs strategic communications, operations, and outreach efforts on behalf of the non-profit. She is an avid traveler, yogi, and foodie. Ms. Chong lives in Sterling, VA, with her husband, adopted dog and cat.



Debra Christofferson has more than 25 years of IT and security management experience, in a Fortune 500 environment, across the United States, Europe, and Asia, with Intel Corporation, the Apollo Group, and the State of Arizona Security and Privacy Office. She has supported security often from the ground up, and worked across multiple lines of business in the public and private sectors in consulting roles. Ms. Christofferson currently serves on the Information Systems Security Association's International Board of Directors and chairs the CISO (Corporate Information Security Officer) Advisory Council for ISSA's CISO Executive Forum. She also leads the local chapter for the Cloud Security Alliance that she co-founded. Christofferson holds the CISSP (Certified Information Systems Security Professional) and CISM (Certified Information Security Manager) security certifications and facilitates local chapter CISM workshops.

Martha Daniel is the founder, president, and CEO of Cytellix and its parent company, Information Management Resources, Inc. (IMRI), responsible for successfully deploying network security and asset management solutions to local, national, and international organizations of every size in a wide range of industries including financial services, healthcare, biotech, education, logistics, and manufacturing. A fearless entrepreneur with 35 years of technology expertise and unsurpassed knowledge of program management and enterprise IT solutions, she is driven by a vision to translate business needs into leading edge technology solutions that help protect customers in both the private and public sectors throughout the world.

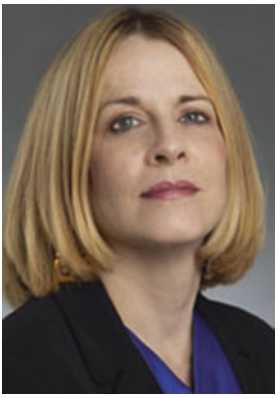
In addition to launching Cytellix, Daniel has led IMRI in becoming an industry frontrunner in cybersecurity, program management, and engineering services for federal and commercial entities, employing more than 155 professionals worldwide and managing over $300 million in data center operations located in 19 U.S. states. Clients include the U.S. Department of the Navy, U.S. Army, and U.S. Air Force, as well as small and mid-size businesses and Fortune 500 companies such as Wells Fargo, Lockheed Martin, and IBM. Prior to IMRI, Daniel had a successful corporate career, serving as chief information officer at FDIC/Resolution Trust Corporation and senior

systems engineer at IBM. She also proudly served as a cryptologist in the U.S. Navy. As *the* unsurpassed authority on the subject of cybersecurity, Daniel's views are regularly profiled across digital, print, and television mediums. She is coauthor of *The Other Side of Midnight, 2000,* has written for *The White House Blog,* and was recently selected as a study group member for the National Infrastructure Advisory Council's (NIAC) Water Sector Resilience Final Report and Recommendations.

Daniel's diligence in inspiring and supporting success in the community has led to keynote speaking engagements at the 6th annual Women as Veteran Entrepreneurs, Irvine Valley College 9/11 Commemoration, and the Biola University's Crowell School of Business MBA Distinguished Speaker Series.

The U.S. Small Business Administration, Santa Ana District Office, selected Daniel as the 2016 Small Business Person of the Year. She was also a recipient of the 2015 Patriot Award given by the Employer Support of the Guard and Reserve (ESGR), established by the Department of Defense. Alongside Chick-fil-A CEO, Dan Cathy, and others, Daniel was honored by the Passkeys Foundation as a 2014 Leader of Integrity for American Life Technology. Additionally, she was honored as one of the top women veteran leaders for the 2014 White House Champion of Change.

A true advocate for change, Daniel contributes her time and resources to various community organizations including the Rothenbuehler Foundation for Veterans, New Directions for Women, the Child Guidance Center, and the Vicksburg Soccer Organization. In addition to being a contributor and guest speaker at the 39th Annual Economic Forecast at Chapman University hosted by James L. Doti, Ph.D., Daniel is also an ordained minister with the African Methodist Episcopal 5th District, a member of the Trusteeship-International Women's Forum, a Vice Chair of the Orange County Business Council Cybersecurity Task Force, and a member of the Orange County Homeland Security Advisory Council. She holds certifications in IBM Project Management and Contract Quality Assurance. A graduate of California State Polytechnic University with a degree in computer information systems, Daniel earned her MBA from the University of La Verne, California.



Mary Ann Davidson is the chief security officer at Oracle, responsible for Oracle software security assurance. She represents Oracle on the board of directors of the Information Technology-Information Sharing and Analysis Center (IT-ISAC) and serves on the international board of the Information Systems Security Association (ISSA). She has been named one of *Information Security*'s top five "Women of Vision," is a Federal 100 Award recipient from *Federal Computer Week*, and was recently named to the ISSA Hall of Fame.

Davidson has served on the Defense Science Board and was a member of the Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency. She has testified on cybersecurity to the US House of

Representatives (Energy and Commerce Committee, Armed Services Committee, and Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology) and the US Senate Committee on Commerce, Science, and Technology.

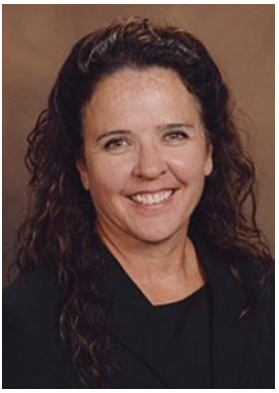
Davidson has a B.S. in mechanical engineering from the University of Virginia and an M.B.A. from the Wharton School of the University of Pennsylvania. She received the Navy Achievement Medal when she served as a commissioned officer in the US Navy Civil Engineer Corps.

Rhonda Farrell is an Associate with Booz Allen Hamilton, primarily focusing on cybersecurity related life-cycle activities within the IC, DoD, and Federal civilian markets. She has led design, quality, and cyber-assurance activities for the federal intelligence and DOD communities aligned with research and development labs, cybersecurity operations centers, and technological infrastructure program management offices. Corresponding areas of focus have been on the introduction of change and quality management principles, process improvement, and supporting strategic planning, risk management, and communication programs. Her prior career experience included operations, engineering, and security functional areas of Fortune 500 companies throughout Silicon Valley, CA, as well as with the U.S. Marine Corps at Quantico, VA.

Her educational background includes a B.S. in Business Administration (heavy Math and C.S.) (1999) and an MBA in Strategic Management (2000) from California State University; a J.D. with a Technology focus from Concord Law School (2009); and is currently preparing for her dissertation defense for her Doctorate of Science in Information Assurance from the University of Fairfax.

She is a veteran committee member and leader within IEEE Region 2, as well as the Northern Virginia and Silicon Valley, CA sections where she has developed initiatives focused on increasing member value, professional development opportunities, section growth, and realization of strategic partnering opportunities. She brings to the section leadership team enthusiasm, a strong work ethic, commitment to IEEE and team-oriented principles, a deep technical background, sound management capabilities, and a solid grounding in cyber and quality best practices.

Rhonda also serves on the International Board of Directors for ISSA—the Information Systems Security Association. She is founder of the Women in Security Special Interest Group (WIS SIG) and leads the SIGS on behalf of the Board. Rhonda is an ISSA Fellow.



Miriam Fernandez currently supports security platform development with Intel Corporation as an Information Security professional in Intel's Key Generation Facility. With 25+ years of experience, Miriam executed multiple IT roles with a global telecommunications and service provider-- Hewlett-Packard (formerly Alcatel Lucent, Lucent Technologies, and AG Communications) for the Americas region. She is an experienced information systems engineer supporting large enterprise IT data centers and networks. These include UNIX servers, and leadership of disaster recovery and business contingency planning programs. She holds a bachelor of science in Computer Information Systems, and earned a Six Sigma Green Belt. Miriam currently serves the Cloud Security Alliance for the local chapter board in AZ and previously was on the leadership teams for the Information System Security Association's (ISSA) Phoenix chapter, and the Sonoran Desert Security User Group (AZ SDSUG).

Pamela Fusco has accumulated more than 30 years of experience as an industry executive and expert in cybersecurity. Ms. Fusco has organized and managed multi-billion dollar global strategic and tactical business driven architecture, technology, and compliance initiatives. She has led numerous global teams to implement innovative business enabling platforms.

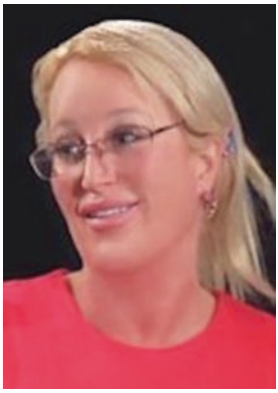
In the past, Fusco resided on the U.S. Presidential White House Inaugural Staff. She has held positions as the chief security strategist; chief information security officer roles with the Apollo Group, Merck & Co., Inc., Digex Inc. (MCI Security Solutions); and EVP of global information security at Citigroup. Pamela was an initial founder of SAFE Bio Pharma Inc., serving on its board of directors.

Fusco began her career in the U.S. Navy serving as a cryptologist, where she supported security proceedings for government and national intelligence and SPECOPS (special operations).

Ms. Fusco has been bestowed with numerous awards and honors including a Presidential Citation, Information Systems Security Association (ISSA) International Hall of Fame, Distinguished Fellow, and Woman of Influence. Fusco is CFO (Chief Financial Officer) of the ISSA International board of directors, contributing author and founding member of the Cloud Security Alliance (CSA), and President, New York Metro CSA Chapter.

Fusco is certificated and accredited as a CISSP, CISM, CHS Level III (Certified in Homeland Security), National Security Agency INFOSEC Assessment Methodology Auditor (AIM Auditor), and National Cryptologic School Adjunct Faculty Certified Instructor (NSA/CSS/NCS) and holds an MS in Information Management.

Ilene Klein For almost 20 years, Ilene Klein has been evangelizing security to anybody who would listen … and to management. During that time, she built and led compliance, governance, incident response, privacy, policy, security awareness, and vulnerability management programs and frameworks. Ilene has earned multiple security and privacy certifications, and she won the CISM Geographic Excellence Award for earning the highest score in the North America geographical region on the December 2011 CISM examination.



Jeani Park is a leading security visionary who has held several executive leadership roles and created bridges to new horizons over the last 20+ years.

Over the course of Ms. Park's career, she developed products in several security areas: AV-anti-spam, network security, wireless security, client server security, mobile security, Internet security, systems management security, endpoint security, and identity management.

Ms. Park is a businesswoman and technologist who has enjoyed a 20+ year career developing, marketing, and monetizing technology products for organizations and consumers around the globe. She enjoys developing emerging technologies that solve real world problems across historically separated domain areas. Ms. Park has worked for companies such as QAD, Access360 (acq. IBM), HP, Dell, Mirage Networks (acq. TrustWave), and Veriato.

During the past fifteen years, Ms. Park focused on digital security, developing products for endpoint security, network security, forensics, user activity monitoring, and security policy and posture. In collaboration with world-class teams and technologists Ms. Park helped build: the integration of on-premise anti-spam functionality with gateway security products (Trend Micro); the integration of hardware and software Systems Management (at Dell); the Network Access Control space (at Mirage Networks); and the User Activity Monitoring space (at Veriato). Ms. Park also had the pleasure of serving as the Cybersecurity Director in the State of Maryland and is a published security author and speaker.

Recently Ms. Park has embarked upon Tech Venture Commercialization work with the University of Utah. Here, she mentors and encourages both tech and science entrepreneurs and researchers to realize success via commercially viable services, products, and companies.

Ms. Park is active in the community as a volunteer and donor for Make-A-Wish Utah, the Leonardo, the National Ability Center, the 1st Lego League,