feature

Balancing the Cybersecurity Battlefield

History shows that women bring a different value to the work environment and improve overall operational effectiveness and financial results. In key financial metrics, companies with women on their boards of directors (BoDs) outperform those without women.[1] Recent research reports that if women were to have economic parity with men in the workplace, global gross domestic product (GDP) could increase by US $12 trillion by 2025.[2] When women are in leadership positions in significant numbers, "the bottom line improves—from financial success to the quality and scope of decision making."[3]

> **"People who think differently because of their gender, culture or training, attack and defend themselves differently and bring unique value to cybersecurity teams."**

Groups are collectively more intelligent than individuals—and that collective intelligence increases as the percentage of women in the group increases, as was learned when women began enrolling in the US military.[4] The military observed that "women provide a vital contribution to critical and creative thinking and decision making in the national security apparatus"[5] and that this capability is missing in many military units where currently there are no women.

Today, the cybersecurity industry is clamoring for women experts, painfully aware that only 11 percent of information security professionals are women, with about 56 percent of those women leaving this sector by mid-career.[6] Women bring specific value to the field of cybersecurity. With half the technology-consuming society being women, a strong representation of women as security practitioners would bring new and deeper insights into the social, psychological, emotional, technical and physical vulnerabilities that attackers are preying on today.

Cybersecurity, in essence, is about protecting information and systems against cyberattacks, cyberterrorism and cyberwarfare.[7] In times of war, governments utilize their entire population to overcome their enemies, often bringing in millions of women to step into roles previously done by men.[8] Excluding women in cybersecurity, where there is a severe skills shortage, is like excluding a battalion in war. It takes all resources to win a war.[9] Cybersecurity is an environment that is about staying ahead of the adversary, protecting assets more quickly than the threat vectors can exploit them, outpacing attackers and applying counterintelligence. Cybersecurity is a battleground of sorts. In war, everything that a country possesses is an asset and used to its own advantage, including the diversity of intelligence, skills and strategy. Women are able to reach the same results as their male counterparts if they get the same rights, privileges and possibilities.[10]

Daksha Bhasker, CISM, CISSP
Has more than a decade of experience in the telecommunications industry working in various roles including business intelligence, strategy planning, business management operations and controls, governance, Sarbanes-Oxley Act compliance, complex technical solutions, security architecture, risk management, and cybersecurity. She is a senior network security architect with the network technology development team at Bell Canada and focuses on the security of emerging technologies.

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

Women should be seen as critical contributors to the cybersecurity industry. Cybersecurity hinges on the three pillars of people, process and technology, all of which can be exploited by attackers. People can be hacked easier than technology. People who think differently because of their gender, culture or training, attack and defend themselves differently and bring unique value to cybersecurity teams. Certain nation-states that are earning reputations as spawning grounds for hackers are not looking for the latest security credential, the most reputed academic degree or a professional licensure to practice in the field. These nation-states are willing to recruit and cross-train on the job. The counterresponse needs to be just as flexible, diverse and prolific. Nontraditional skills are important to the cybersecurity industry. For example, a political scientist may have insights into the agenda of nation-states and strategies that can be augmented to understand the motive and means of an attack. Similarly, a psychologist can offer threat intelligence that is based on human behavior and analysis. In cybersecurity, diversity brings value and expands the strength of the team.

> **“As career participation and advancement becomes a challenge, dissatisfied women tend to opt out of cybersecurity mid-career.”**

Women can face numerous barriers to entry into the cybersecurity arena. Security industry opportunities that are commonly denied to women include:

- Inclusion in the cybersecurity community
- Equal opportunities for training and skills development
- Peer acceptance
- Acceptance as leaders
- Acceptance as engineering and technical experts
- Career advancement opportunities within the security industry

The present community of security professionals is a well-established, predominantly male community.[11] It takes extraordinary grit and effort for newcomers, especially women, to penetrate these networks. They face reluctant inclusion as they strive for acceptance by the community and hope that, at some point, their security careers will flourish. They seek equal participation opportunities, acceptance and integration. This is reflected in the meager 10 percent of information security leadership roles that are occupied by women today.[12] Cybersecurity is unique because it is a community of secrets, secret knowledge, classified information, association with dark hacker communities, trust circles and other secret resources. Security intelligence organizations around the world extol secrecy as their primary strength. A secret, by definition, is the exclusion of others in information sharing. Exclusion in the cybersecurity community can happen to anyone who does not fit the typical profile, including women.[13] Government security clearances do little in advancing women into security information professional circles, even when working around security communities in security organizations. This lack of advancement results in a high percentage of women being relegated to security-related essential, yet ancillary, functions such as administration, project or program management, business development, and marketing or communications. Because women often work in these roles, some may never quite penetrate to core security roles.[14] As career participation and advancement becomes a challenge, dissatisfied women tend to opt out of cybersecurity mid-career to areas where upward mobility is more accessible.[15]

Security professionals are rarely the most popular experts in a company regardless of gender. Most projects and initiatives consider security requirements to be impediments or necessary and painful overhead. Security professional expertise, opinions and budget requirements invariably experience responses of aggressive scrutiny and rigorous uproars, often by nonsecurity professionals.[16] Women have a tendency to overcompensate for being in a male-dominated field, a phenomenon referred to as the Madame Curie effect, meaning that women believe they must become more qualified and develop exceptional ability to compete with men in male-dominated science.”[17] This tendency, combined with the previously mentioned roadblocks, is especially taxing and has an effect on women who are developing new skills and working up a cybersecurity career path.

When work-related social events are male-dominant events, despite the best of intentions, women can continue to feel marginalized and struggle to bond with their cybersecurity colleagues. These situations can alienate and isolate a woman cybersecurity professional who does not have stereotypical male interests.

Aside from the very basic requirements of work-life balance and equal pay, there are a host of things that can be done to support, encourage and retain women in cybersecurity. The following efforts can help encourage women to participate in cybersecurity and advance toward leadership positions:

- Invitations and welcomes for women as professionals and allies into the field
- Open information sharing
- Training
- Career coaching
- Support
- Respecting differences in opinion based on professional background
- Partnership with mentors

The following steps can help to better incorporate women into the cybersecurity workforce:

- Make clear attempts to diminish the male-dominated stereotype of the cybersecurity industry. Both men and women are needed to win the cybersecurity fight. The image of cybersecurity professionals is predominantly male in the media. Overhaul such widespread imaging from hoodie-clad, keyboard pounding, acrobatic male ninjas to one of professional business etiquette, elegance and standards. Ensure a similar professional work climate where women can thrive in work-related social events as much as their male counterparts.
- In the workplace, welcome women as they develop subject matter expertise in core cybersecurity roles. Ensure a space of respect among all employees, especially those who do not have a history of working with women as peers and leaders.
- Encourage women by taking an active interest in their cybersecurity careers. Offer equal access to training and help eliminate barriers where women wish to pursue and sustain careers in cybersecurity. Provide access to professional networks and mentoring. Develop a discipline-specific mentor match program for women and offer established industry mentors for as long as this support is needed. Be aware of the Madam Curie effect and utilize mentoring as a channel to reduce this tendency. Encourage women, especially leaders in technology and engineering, to nurture newer entrants in the cybersecurity domain.
- Incentivize women to achieve leadership roles in cybersecurity and set clear paths of promotion for women employees. Enterprises can begin by maintaining transparent statistics on gender distribution in cybersecurity, tracking them against desired benchmarks. Communicating these statistics openly, while measuring them annually for progress, increases awareness of the gender-distribution gap and spurs desire for remediation. Reward women with financial incentives or incorporate recognition for attempting a nontraditional career in cybersecurity, and monitor their progress year after year. Create pro-women cybersecurity interest groups, networks and forums to enable women to have easy access to support, guidance and information. Establish exit interviews for women who choose to leave the field to understand and address identified shortcomings. Engage managers in attracting and retaining women employees.

- Manage the culture of secret intelligence and required nondisclosures that is prevalent in the security industry with as much openness and transparency as possible. Help to prevent the misuse of information classification systems to prevent unnecessary exclusion of newcomers to the cybersecurity field. Create a mechanism that challenges such exclusion and openly discuss how to prevent this exclusion. Promote the need for training in the workplace to overcome unconscious biases against women in this industry.

Collectively, the goal of cybersecurity professionals is to win the cybersecurity war against attackers. Let women in the arena know that cybersecurity is their fight, too. Women on the cybersecurity battlefield are an asset.

Acknowledgement

The author would like to thank Tyson Macaulay, chief security strategist and vice president of security services at Fortinet, for many years of mentorship, guidance and shared insights.

Author's Note

Opinions expressed in this article are the author's and not necessarily those of her employer.

Endnotes

1 International Labour Organization, "Women at Work: Trends 2016," International Labour Office, Geneva, 2016, *www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/---publ/documents/publication/wcms_457317.pdf*

2 Woetzel, J.; A. Madgavkar; K. Ellingrud; E. Labaye; S. Devillard; E. Kutcher; J. Manyika; R. Dobbs; M. Krishnan; "The Power of Parity: How Advancing Women's Equality Can Add $12 Trillion to Global Growth," McKinsey Global Institute, McKinsey & Company, September 2015, *www.mckinsey.com/global-themes/employment-and-growth/how-advancing-womens-equality-can-add-12-trillion-to-global-growth*

3 Seliger, S.; S. L. Shames; *The White House Project Report: Benchmarking Women's Leadership*, White House Project, USA, 2009

4 Haring, E. L.; "Women in Battle: What Women Bring to the Fight," *Parameters*, vol. 43, iss. 2, 2013, p. 27

5 *Ibid.*

6 Frost & Sullivan, "Agents of Change: Women in the Information Security Profession, The (ISC)^2 Global Information Security Workforce Subreport," *www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/Women-in-the-Information-Security-Profession-GISWS-Subreport.pdf*

7 Palo Alto Networks, Inc.; "What is Cyber Security," 2016, *www.paloaltonetworks.com/documentation/glossary/what-is-cyber-security*

8 Kabanenko, I.; *The Importance of Effective Utilization of Women at Arms*, Naval Postgraduate School, USA, March 2015

9 Online Highways LLC, "Rosie the Riveter," u-s-history.com, *www.u-s-history.com/pages/h1656.html.*

10 Rayman, N.; "Female Chess Legend: 'We Are Capable of the Same Fight as Any Other Man'," *TIME*, UK, 20 April 2015, *http://time.com/3828676/chess-judit-polgar-nigel-short-sexism/*

11 *Op cit,* Frost & Sullivan

12 *Ibid.*

13 D'Hondt, K; *Women in Cybersecurity*, Harvard Kennedy School, USA, 2016

14 *Op cit,* Frost & Sullivan

15 Morbin, T.; "RSA: Women Breaking the Glass Firewall," *SC Magazine UK*, 21 April 2015, *www.scmagazineuk.com/rsa-women-breaking-the-glass-firewall/article/410089/*

16 Sethi, R.; "Managing Security Requirements in Agile Projects," *InfoQ*, 4 June 2012, *https://www.infoq.com/articles/managing-security-requirements-in-agile-projects*

17 Natural Sciences and Engineering Research Council of Canada, "Women in Science and Engineering in Canada," November 2010, *http://publications.gc.ca/collections/collection_2012/rsgc-serc/NS3-46-2010-eng.pdf*