Breaking the Firewall to Girls' Cybersecurity Access

Summary

Cybersecurity is one of the top risks that companies and individuals alike face, and it affects every aspect of our lives. From the integrity of our elections to the safety of our infrastructure, to the protection of our data and even our identities, we are all vulnerable to cyberattacks from criminals. Unfortunately, as they become increasingly sophisticated and use advanced methods and technologies, we grow closer to a massive shortage of experienced cybersecurity expertise, with millions of cybersecurity jobs estimated to be unfilled in the next few years.

At the same time, women are grossly underrepresented in cybersecurity and hold a minority of leadership roles within the field. This is significant for many reasons, not the least of which is that women are more likely than men to be sexually harassed and stalked online. Children are also vulnerable and can fall victim to online predators, suffer cyberbullying by their peers, or unwittingly compromise their privacy by using popular apps.

One solution to both the shortage of cybersecurity experts and the need to better address women and children's unique vulnerabilities in cyberspace is to bring more women into the field—particularly leadership roles. To achieve this, we need to create a strong future workforce by educating girls about why cybersecurity matters and giving them the skills they'll need to pursue careers in the field. As the preeminent leadership development organization for girls, Girl Scouts is perfectly positioned to accomplish this goal.

In 2018, Girl Scouts of the USA (GSUSA) partnered with Palo Alto Networks to add Cybersecurity badges to Girl Scout programming. Then, in 2019 and 2020 we also partnered with Raytheon Technologies to host a Cyber Challenge (a nationwide event through which thousands of girls solved a hypothetical ransomware attack). Through our programs, girls are empowering themselves with the knowledge, skills, and hands-on experience necessary for them to thrive in the interconnected world we live in and to become the cybersecurity leaders of tomorrow.

This paper explores these ideas, offering research as well as insight from two leading cybersecurity experts on the current state of play as well as next steps.

> “It was the confidence I developed as a young Girl Scout that gave me the courage to do something that not a lot of girls were doing at the time. In my case, it was engineering; for this generation of girls, it will be cybersecurity.”
>
> **Sylvia Acevedo**
> GSUSA CEO

Table of Contents

I. Key Statistics on Cybercrime

- The World Economic Forum's *Global Risks Report 2019* ranked massive data fraud and theft as the fourth biggest global risk (after extreme weather events, climate change, and natural disasters). Cyberattacks ranked fifth globally and first in Europe and North America.

- According to *Ponemon Institute*, 90% of all critical infrastructure providers say their information technology and operational technology (OT) environments have been damaged by a cyberattack in the last two years, and 62% experienced two or more attacks. OT runs the physical systems behind planes, trains, ships, traffic systems, and the power grid.

- Within the first nine months of 2019, 7.9 billion records containing sensitive information, including financial and health details, were exposed in North America, more than doubling the number exposed during the same period the year before.

- Public and private organizations experienced an average of 145 security breaches in 2018—an 11% increase from 2017 and a 67% increase over the past five years, according to the *Cost of Cybercrime Study* from Accenture and Ponemon Institute.

- The average total cost of a data breach rose to $3.86 million in 2018, according to Ponemon Institute's *2018 Cost of Breach Report*.

- Data breaches are predicted to cost the world $5 trillion annually by 2024, according to Juniper Research.

- Ransomware attacks (malware that locks or denies access to a computer's files until a ransom is paid) are on the rise and expected to increase, especially within local municipalities. These attacks spread through phishing emails, infected websites, and external sources, such as thumb drives.
  - More than 70% of ransomware attacks in the United States target state or local governments.
  - A ransomware attack shut down Atlanta's city hall for five days in 2018—disrupting critical city services and operations at Hartsfield-Jackson Atlanta International Airport at a reported cost of $17 million.
  - A 2018 ransomware attack in Baltimore paralyzed the city's 911 emergency call center, and a second attack in 2019 took over the city's computer systems. The latter attack cost an estimated $18.2 million.
  - In 2018, 22 Texas towns were hit by coordinated attacks and had their systems held for ransom; in one town alone, hackers demanded $2.5 million to unlock the files.

- In 2017, the global cost of cybercrime was an estimated $600 billion, or 0.8% of global GDP.

- By 2021, cyberattacks are predicted to cost the world $6 trillion annually, according to Cybersecurity Ventures.

II. Shortage of Cybersecurity Experts

As governments and organizations attempt to keep pace with cybercriminals—who work with increasingly sophisticated methods and technology—these entities are hampered by a shortage of cybersecurity professionals. The shortfall is exacerbated by the deficit in all science, technology, engineering, and math (STEM) workers. According to a study by the National Association of Manufacturing and Deloitte, the United States will have to fill 3.5 million STEM jobs by 2025, and 2 million of those will remain unfilled because there aren't enough qualified workers. When looking more specifically at the number of cybersecurity professionals available, the shortage is even more pronounced. Put simply, there's a cybersecurity arms race, and right now we're losing.

It's not just lost revenue, tax dollars, and intellectual property at stake, however. The nation's critical infrastructure, including the power grid, is also vulnerable to cyberattacks. Equally important, virtually every aspect of our lives is now online—from our bank accounts and health records to our cars and refrigerators—and all those systems can be hacked. Because they've been digitized, cybercriminals can access them and assume total control.

A skilled cybersecurity workforce, therefore, is an economic, safety, privacy, and security imperative.

III. Lack of Women in Leadership Roles

It's no secret that women and people of color are underrepresented in STEM fields. Overall, women comprise half of all STEM workers in the United States, but the share of women working in STEM occupations varies greatly across fields and education levels (2018, Pew Research Center). Women account for 75% of workers in health-related jobs, for example, but only 14% in engineering. And although computer science jobs have grown a staggering 338% since 1990, women's representation has actually decreased—from 32% in 1990 to 25% in 2016. Perhaps unsurprisingly, the largest gains for women in STEM jobs are among those with advanced degrees.

This underrepresentation is drastic in cybersecurity, where women comprised only 11% of the cybersecurity workforce worldwide from 2013 to 2017. The *2019 Women in Cybersecurity report* from the International Information System Security Certification Consortium (ISC)2 found that the number has risen to 24% but noted that a revised methodology (which took a more "holistic look at who is truly doing the work of cybersecurity") likely accounts for the increase. In any event, the number is still strikingly low, considering that women make up 39% of the global (and 46% of the U.S.) labor force.

The (ISC)2 report also found that women in cybersecurity continue to earn less than their male counterparts at nearly all income levels and among every generation (Millennials, GenXers, and Baby Boomers). Globally, the gender pay gap is less pronounced among younger women, with the greatest disparity among Baby Boomers.

Another study that analyzed compensation for 15 IT and security certifications found a gender pay gap ranging from 2% to 18%, depending on the job, with women earning an average of 8% less than men. This may seem negligible until one considers that the salary for a chief information security officer is $173,449 and can top out at nearly $300,000.

IV. Women and Children's Unique Cybersecurity Needs

The lack of female representation in tech has created huge blind spots in certain technological applications. For example, when the Apple Health app was first released in 2014, it allowed users to track a diverse amount of health data but had one glaring omission: menstrual cycles. The app ignored one of the most important aspects of health for half the population simply because there were no women in the room when it was developed. Likewise, a number of other fitness apps and products originally didn't take into account gaining weight during pregnancy, breastfeeding, or even pushing a stroller while walking.

Similarly, the few women in cybersecurity means their needs aren't sufficiently considered, let alone addressed. We've seen this narrative play out before, particularly in medical research and healthcare, both of which have traditionally been dominated by men. We now know, for instance, that cardiovascular disease, Alzheimer's, and lung cancer all affect women differently than men, yet for years women were either excluded and/or underrepresented in research studies—or gender was not taken into consideration at all. This gender bias has often led to poor health outcomes for women.

Because women experience the internet differently than men, they're more concerned about online privacy than men—and with good reason. Women and children face a drastically different online environment:

- According to Pew Research, women are more likely to be sexually harassed online, and they're twice as likely to say they have been targeted because of their gender. Additionally, the Justice Department reports that around 75% of stalking and cyberstalking victims are women.
- A majority (59%) of U.S. teenagers have experienced some sort of cyberbullying, and 90% believe online harassment is a problem affecting their age group.
- In September 2019, Privacy International reported that several period-tracking apps were sharing millions of users' highly sensitive information with Facebook and other third parties, including—in the case of two apps—when users last had sex.
- Smart home technology is increasingly being harnessed as a weapon by domestic abusers who monitor and control those they abuse, the majority of whom are women.

Most troubling of all, social media and encrypted networks have enabled predators, including pedophiles, to target children and share abusive images. In 2018, tech companies found more than 45 million online photos and videos of children being sexually abused, double the number from 2017.

The fact is, women and children have different needs and are considerably more vulnerable online than men. The lack of female representation in tech and cybersecurity has led to dual outcomes: 1) much of the tech being developed doesn't take women's needs and wants into account, including vital safety and privacy concerns, and 2) the rules that govern internet and social media use have failed to protect women and children from exploitation and harm.

The fact is, even while women make up half of the internet's and social media platforms' users, they're underrepresented among those who create the rules and privacy guardrails that make using digital technologies a safe experience. The lack of female representation in tech and cybersecurity has meant that much of the tech being developed doesn't take women's needs and wants into account, including vital safety and privacy concerns.

V. Why We Need More Women in Cybersecurity

One solution to both the shortage of cybersecurity experts and the need to address women and children's unique issues is to not only bring more women into cybersecurity but to increase their numbers in leadership roles. Cybercriminals are not a homogenous group; they come from a wide variety of backgrounds and geographic locations and bring diverse skillsets and experiences. Therefore, to combat them, we need an equally diverse cybersecurity workforce.

The 2019 (ISC)^2 report found that women value cybersecurity or related graduate degrees more than men (28% vs. 20%). In fact, 52% of women in cybersecurity hold a master's degree or higher, compared to 44% of men, and women generally earn more cybersecurity certifications. Additionally, women working in cybersecurity have a more varied educational background than men, contributing to the diverse skillsets the industry so desperately needs.

Beyond needing women's valuable perspectives, we need their talent and expertise. As we face the enormous shortage of skilled cybersecurity experts—which is expected to worsen in the coming years—we can't afford a brain drain in this critical area. It's not simply a matter of protecting individuals from hacking or data theft, and it's not merely keeping ransomware out of our local governments; cybersecurity is the new battlefield, and to win the arms race, we need all hands on deck.

Speaking at an event in October 2019, Jeanette Manfra, then–assistant director for cybersecurity for Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), said that the lack of cybersecurity professionals and skills shortage in the private and public sectors are a threat to national security.

To get a clearer picture of the climate for women in the industry, why we need to increase their numbers, and how to achieve that goal, we consulted two cybersecurity experts. Their perspectives follow.

Tyler Cohen Wood Tyler Cohen Wood is the former director of cyber risk management for AT&T and was the deputy division chief of the Defense Intelligence Agency. She has been a senior intelligence officer and worked with the White House, Department of Defense, federal law enforcement, and the intelligence community. Tyler is also the founder of Cybergirlpower.

Currently, the ratio is so skewed toward men, there have been many times during my career where I felt like I was in an old boys' club where women were pushed out. This affects what is being developed and whose voice is being listened to. We have to have diversity and inclusion; we cannot just have one single point of view.

Oftentimes with new technologies or products, security is pushed to the side because the developers or companies want to get them to market faster. When women look at security, it's more organic to a product rather than an afterthought. With the women that I've had the pleasure to work with, they want to put in more security measures, even if it makes things slightly less convenient. For example, doctors can view your medical information on their tablets or phones. They can look at test results and write prescriptions, which is convenient, but it's incredibly easy to hack one of those devices. I think women would have put security first and maybe made it a little less convenient because they understand the need to protect our digital records and, particularly, information about our children.

Girls need to have a community available to them where they see strong female leaders in tech and see how much can be achieved. They also need to get hands-on experience. It's one thing to talk about the different tools and technologies, but girls need to know the security risks behind the technology they're using. For example, they know that if they send a photo on certain platforms, it's supposed to disappear, but what they don't know is that the photo i sn't necessarily gone. They understand the technology, but they don't really understand the security behind it.

By having more initiatives where girls are getting hands-on tech experience, they're learning the hacks and learning how to do all these cool things in a very supportive environment with other girls who are doing the same exact thing. It inspires them. It empowers them. It helps them to see, "Oh, my goodness, I can do this and I'm good at this, and I want to do this." And an important aspect is that they are getting the experience in girl-only environments. Aside from my talent, my initiative, and my drive, there are two things that I think helped me get into this career and excel at a time when it was all men. The first was that I went to an all-girls' high school and the second is that I graduated from an all-women's college. That really helped me because I had a level of confidence that I'm not sure I would have had if I had gone to a school that was boys and girls.

John Sileo got started in cybersecurity 15 years ago when he lost everything, including his $2 million business, to cybercrime. John is the founder and CEO of the Sileo Group, a privacy and cybersecurity think tank, and an award-winning author; keynote speaker; and expert on technology, cybersecurity, and tech/life balance.

Cybersecurity is what keeps organized crime out of our life savings; rogue nation states out of our nuclear power plants and hospitals; and dictators and overzealous corporations out of our bedrooms, voting booths, and psychographic profiles. Not having the experts is like not having the soldiers at Normandy—technology is the new marketplace, the new battlefield, the new political podium. Cybersecurity is what defends all of those institutions.

Regarding women in cybersecurity, diversity inside of any organization on any topic increases innovation. In security, women are vastly underrepresented, so there is more of the "defend the castle" attitude (male) than "this is important; let's collaborate and figure it out as an organization, not as a siloed security function" (female). This causes an implicit bias in the way security is approached.

The traditional and still pervasive "defend the perimeter" approach to protecting data inside an organization is the byproduct of a male-dominated workforce. We are now seeing much more in the way of defending from the inside out, educating our people, caring about what happens to them and their data first, and then leveraging that into a culture of security that is organic and extends to the perimeter and beyond. In my opinion, the perimeter is an outdated concept and yet firmly held on to by many security professionals (mostly men, to date whether due to attitude or just to a more weighted representation).

When we close the gender gap, everything will improve, just as I have improved as a person having had a strong wife and two daughters educate me on perspectives I would have NEVER entertained otherwise. Just as I am a vastly different person today because of the leadership of women in my life, so will the cybersecurity community be different for having that diverse perspective.

I'd like to see more young women and girls take an interest in technology and the security behind that technology and be rewarded, incentivized, and educated to do so.

We need to start educating and training girls at a young age to level the playing field BEFORE they step into it. I think that the neurological diversity that women (and other underrepresented groups) bring to the field depends on them having risen through the ranks, just like they do in sports, academics, or art. Security is a tangible, trainable, attainable thing, but you need to incorporate diverse perspectives to make cybersecurity a reality.

VI. How to Bring More Women into Cybersecurity Leadership Roles

Because the shortage of skilled cybersecurity professionals is tied to the shortage in STEM workers, we cannot address the former without addressing the latter. According to the Girl Scout Research Institutes' 2019 report *Decoding the Digital Girl*, girls' interest in STEM fields peaks in middle school and decreases in high school. (Notably, the drop is less significant among Girl Scouts than non–Girl Scouts.) The same study found that 32% of girls ages 5–17 are unfamiliar with cybersecurity as a tech field.
This last finding suggests a disconnect between girls' use of technology and their awareness and appreciation of cybersecurity. A recent study from Common Sense Media found that tweens spend four hours and 44 minutes per day on a screen, and teens spend seven hours and 22 minutes per day—not including the amount of time either group spends on a screen at school or doing homework.

This screen time also doesn't include the myriad ways that cybersecurity intersects the lives of tween and teen girls on a daily basis, including through their families' smart home devices and smart cars, as well as the online digitalization of their school and health records.

A 2017 survey commissioned by Raytheon, Forcepoint, and the National Cyber Security Alliance found that the majority of Millennial women say they would have been more interested in a cybersecurity career if they'd had access to more information about it and training in STEM during middle and high school.

The first step toward a solution is to educate girls at a young age about why cybersecurity should matter to them and to inspire them to be the cybersecurity leaders of tomorrow. We then need to support them with the training, mentoring, and hands-on experiences they'll need to assume those leadership positions.

Encouragingly, the (ISC)^2 report found that 45% of female cybersecurity professionals surveyed are Millennials, compared to 33% of men. With Generation X, the split was 44% men to only 25% women, meaning that younger women are entering the field at higher rates than before. These women represent an important shift in the right direction and will be crucial role models for other women, including those from future generations.

VII. Girl Scouts Is Leading the Way

For decades, Girl Scouts has been innovating in extracurricular STEM education through programs aimed at increasing girls' interest, confidence, and competence in STEM. Our programs give girls the training, mentoring, and hands-on experiences to help them understand the value of STEM to society and the options for their own related career paths. And it works! Our research shows that Girl Scouts are more likely than non-Girl Scout girls to be interested in STEM and careers in tech—including app development, robotics, coding, and cybersecurity.

In 2017, we pledged to add 2.5 million girls to the future STEM workforce by 2025. The goal is simple: to ensure that girls are prepared with the skills and experiences to become the STEM leaders of the future. In 2017, Girl Scouts launched computer science Think like a Programmer programs for girls in grades K-5 and in 2018, Girl Scouts collaborated with Raytheon Technologies to introduce Think Like a Programmer programs to older girls in grades 6-12. In 2019, Girl Scouts collaborated with Dell and AT&T to introduce Coding for Good badges for girls in grades K-12.

As an extension of our commitment to prepare girls for careers in STEM — and in recognition of the monumental shortage of qualified cybersecurity professionals and the need to bring more women into the field — in 2018 Girl Scouts of the USA partnered with Palo Alto Networks to introduce cybersecurity badges to girls in grades K–12. The national effort was a huge step toward eliminating traditional barriers to industry access, such as gender and geography, and targeted girls as young as five years old, helping to ensure that even the youngest girls have a foundation primed for future life and career success.

By May 2020, Girl Scouts earned more than 1 million STEM badges, including more than 150,000 Cybersecurity badges.

We've also partnered with Raytheon Technologies to host our first Cyber Challenge for middle and high school girls. The 2019 pilot event reached thousands of girls who learned about cybersecurity and got direct experience through fun and engaging activities that exposed them to computer science and cybersecurity topics such as cryptography, forensic analysis, encryption, decryption, and hacker tracking. In 2020, Girl Scouts is continuing to collaborate with Raytheon Technologies on a national Cyber Challenge where girls solve a hypothetical ransomware attack.

Since 1912, Girl Scouts has been the preeminent leadership development organization for girls, with a research-backed program that cultivates their ability to learn and grow in a safe, all-girl environment in which they discover who they are, connect with others, and take action to make the world a better place. Through our programs, girls are empowering themselves with the knowledge, skills, and hands-on experience they need to thrive in the interconnected world we live in and to become the cybersecurity leaders of tomorrow.

The Girl Scout Research Institute delivers data-driven insights across the Girl Scout Movement and beyond, leading national conversations about girls and their development via groundbreaking original studies.

The Girl Scout Research Institute
Girl Scouts of the USA
420 Fifth Avenue
New York, NY 10018
gsresearch@girlscouts.org