11% is Not Enough. Deborah Hurley on Why Women Should Join Cybersecurity

INTERVIEWER:
Welcome to the Brown Executive Master in Cybersecurity podcast series. In this interview, we tackle the issue of women in cybersecurity with Deborah Hurley, a professor in the Brown Executive Master in Cybersecurity program. Deborah starts off by informing us that women actually went into computer science during this field's infancy. She then ponders why we jumped off this gravy train and continue to shy away from math and science oriented sectors that are the greatest wealth engines of our time.

While this all sounds very gloom and doomish, I encourage everyone to listen to this podcast because she then explains how cybersecurity is inherently interdisciplinary and offers a path for a broad array of professionals who want to join one of the biggest growth areas of our economy. So if you're in education, administration, technology, health care, insurance, the legal profession, and much more, listen to this podcast to find out how your voice is critical in the build out of the cybersecurity sector. We begin this podcast asking Deborah, why are there so few women in cybersecurity today?

DEBORAH HURLEY: There are very few women in cybersecurity. And it's not only a problem in cybersecurity, but more broadly in science and technology and mathematics, generally. So there are several problems here. And they apply to that broad field and also to cybersecurity. And the problems are interrelated.

The threshold problem is that there's been a precipitous decline in women going into math and science subjects. So that's been going on for years. It's disastrous if you look at the numbers.
Biology is a small bright spot. But otherwise, we see women self-selecting out of math and science subjects. Initially, when computer science began as a field, there was a slight rise and initial blip of women going into this new field. But then again, it followed very quickly the same precipitous crash of women going into science and technology, including cybersecurity. So that's problem number one. So women are staying out of and not going into an important, interesting, growing, dynamic area of the academic world, the economy, and the society. So that's a big problem.

And then the situation assumes disastrous proportions when you consider that by self-selecting out of science and technology, women have closed themselves off from one of the biggest engines of wealth creation in our era. Compounding that already shocking state, the number of single parent families is growing in the United States. So single parent families is a euphemism for women raising their children by themselves. So the women and their children are excluded from wealth creation. That is when this assumes the proportions of a tragedy. That's problem number two.

Now, for problem number three. Some women do go into science and technology fields. Then when they get there, they encounter an all-male, or virtually all-male environment, or a cliff of discrimination, which they must scale. For example, the percentage of women in Silicon Valley is minuscule compared to the fact that, obviously, women are 50% of the population.

I'll give you a personal example. When I started my working life in advanced science and technology policy, I was often the only woman in the room, whether the room had 50 people in it, 5 people in it, or 500 people in it. That was quite typical at that point. But to my surprise, there has been little change over the years.

A few years ago, I was working-- I realized at one point that I was working with five different organizations on five different high-tech issues in five
different sectors. This group of five included a large academic consortium, which I was running, and a few startup companies across the gamut in terms of sectors. They ranged in size from about 5 to approximately 26 people. I realized that I was the only woman involved in any of these organizations.

There are numerous other examples that swim through the popular press--Gamergate, litigation about discrimination. Recently, women in Silicon Valley announced that they had formed a nonprofit group to try and increase the number of women in high tech fields.

So what happens here? Some women drop out. Other women hang in there, but they don't receive the same recognition, training, or opportunities as their male colleagues. So that's problem number three.

There are counterpoints to this. There's a relatively new field of chief privacy officers and others working in the privacy field. And that has attracted many women to it. So these women are dealing with many issues related to new technologies because a lot of the privacy-related issues today result from burgeoning new technologies and implementations. But, there is a concern that wages in a field tend to decline as it comes to be perceived as a woman's or a female profession. So this is something that we need to be vigilant about not only in the privacy field, but more broadly.

So all of this that I've described very briefly here turns into a self-reinforcing cycle or a self-fulfilling prophecy for the individual woman. We, and I mean every human being including women, must break these cycles. Women must reach out to other women and women should join local, national, and international organizations that have a mission to support women in their professional fields. And if there isn't one in your area, set one up immediately.
INTERVIEWER: Well, that ended on an optimistic note. But you painted a pretty bleak picture before that. Can you identify some bright spots in the field of cybersecurity for women?

DEBORAH HURLEY: Yes. Absolutely. I, obviously, am very interested in computer security. It's a field I've been involved with for many, many years-- really from the beginning. So in the cybersecurity area, it is not only, first of all, about science and technology. That's just one component of it and not in the least or by any means the whole picture. Cybersecurity itself is inherently interdisciplinary and multi-stakeholder.

So in 1989-1990, quite some time ago, I wrote the first comprehensive report on security of information systems, as we called it at that point. Now, it's generally called cybersecurity. So before that time, there existed a few technical manuals on computer security. For example, there was something called the Orange Book that the United States government had produced, which covered only technical matters related to computer security.

The report that I wrote looked across the entire horizon of computer and communications security and included not only technical issues, but also and equally importantly, management, legal, and other issues. In fact, one of the key points of the report and something which is viewed as axiomatic is that cybersecurity will not happen or will not happen sufficiently without senior management support and attention.

It's typical that people who are similar to each other like to talk and work together. So the computer scientists want to work with the computer scientists and the lawyers want to get together and consult with the lawyers. But in order to address cybersecurity problems in a robust, sustainable manner, it's essential to confront them in an interdisciplinary way, pulling what's best and the needed tools from the entire arsenal,
whether they be technical, legal, management, or other, and to use them in combination to meet the security challenge.

Many cybersecurity problems have little to no technical component. In fact, the biggest cybersecurity problems come from human beings. So the effective management and training of people is essential. When we talk about human vulnerabilities, the popular imagination runs to malicious hackers and cyber criminals. And they certainly exist and are a problem. But in fact, what most people don't realize is that the biggest cybersecurity issues come from employees, and not from the disgruntled ones, but from the employees who are well-intentioned, happy employees, but are fatigued, negligent, or insufficiently trained.

Cybersecurity is absolutely a multi-stakeholder undertaking, meaning that people from diverse backgrounds have to come together to solve problems. Cybersecurity is a big tent with lots of different kinds of people in it.

So the ability to get along with, bring together, supervise, and get results from a broad range of people is an absolutely vital skill. Furthermore, it's useful to be able to understand and manage human and social behavior among employees, customers, and clients, and with the public at large.

Cybersecurity is a growing field, absolutely, with lots of jobs and opportunities. And I strongly encourage women to take a look. Whatever a woman's talent, whether it's with people, technology, administration, management or education, there is very likely an aspect of cybersecurity for which her skills and expertise are needed. In addressing cybersecurity issues and in working with colleagues from many disciplines, which will be a daily part of working life, these women will grow in their own knowledge, experience, and expertise, and thereby make themselves more expert and more able to contribute to the workplace and to the economy and society.
**INTERVIEWER:** Well, it's great to hear that there are so many avenues for people to enter cybersecurity. What advice do you have for women who want to enter this field?

**DEBORAH HURLEY:** I guess I'd give the following advice. And this is for women at all ages or all points in their career. These things remain evergreen, and it's good to revisit them from time to time.

I guess I would start with Henry James' famous statement about how do you succeed in the world, or how you succeed in business. And to paraphrase slightly, he said, be kind, be kind, be kind. I think that's very important. Secondly, I would advise women strongly to have their own source of income, which means that you have a skill or, better, several skills that the marketplace wants to buy. And please remember, those single parent families -- in other words, those women raising their children alone -- also have your own source of income.

Third, be ruthless with your time. People want to occupy your mental real estate and use it for free. It's very important to really be directed about how you apply your time and what you spend it on. Next point, set goals and walk relentlessly toward them. Have a five-year plan. Have a three-year plan. Whatever it might be.

Another point that's very important is to find mentors and ask them to help you. Just recently, a woman came up to me in a conference-- and this is not the first time this has happened. And she came up to me. We'd met briefly over coffee earlier in the day. And I'd given a talk. And she came up and she said, “Will you help me? I really want to just shift and make a transition in the work I'm doing.” And I said absolutely, yes. So people are open to that. Older women definitely feel, as they move on in their career, an obligation to reach out a hand to women who are coming up behind them. So please, all of us, look for mentors and ask them to help you.
Then also, say no and say yes. You need to be able to say no. And that's a skill that women need to develop. Women often say they have trouble saying no. You must say no. But you must learn to say it gracefully. On the flip side of that, you need to say yes. And that means being really open to opportunities. You're laying the field. You're preparing a field and fertilizing it with the kind of information you're gaining, your experience you're gaining. And so when those opportunities come your way, leap for them, say yes to them.

I would say form rich networks with all kinds of people, in the enterprise and in your communities. And then with regard to cybersecurity specifically, all of those apply to that field.

I will tell you it's a fascinating field with lots of important work still to do. It impacts just about every economic and social sector that you can possibly think of. If you think you may be interested, I urge you to learn more about it. Think about the skills you have or can develop and that you can bring to the party to help us with the problems in this field. Please come join us.

INTERVIEWER: That was fantastic advice. Thank you for sharing your thoughts with us. Thank you for listening to this podcast. For more information on future podcasts, program news, and upcoming events, please visit brown.edu/cybersecurity.