Season 2: Cybersecurity Education and Diversity in Higher Education
Guest: Dr. Bhavani Thuraisingham
You Got Hacked
Bhavani's answers to the Podcast organized by Sierra Neveda Corporation
December 6, 2022

PART 1

The field of cybersecurity is all encompassing, and the people who work in this field can come from many different walks of life. One way people first get involved with this complex subject is through education. Our teachers, educators, and professors are the first light that sparks for many people to study, learn, and grow in computer science, engineering, and cyber security.

On You Got Hacked, we are doing a mini-series focusing on cyber security education and the role that education can have to hopefully inspire the next generation of cybersecurity warriors. This will be part 1 of 2 where we'll explore Dr. Bhavani's insights from over 35 years in the cyber world.

Dr. Bhavani, welcome.

Ariel: Dr. Bhavani, thank you for joining us today on You Got Hacked. Please introduce yourself to our listeners.

Dr. Bhavani: [Self-introduction]

I am Dr. Bhavani Thuraisingham Founders Chair Prof. of CS and founding exec director – women in cyber sec and data science. I have a 37 yr. career in cyber security and have worked at commercial Honeywell, MITRE, NSF, and UT Dallas. In addition to my technical work and awards, I have also written opinion and other articles as well as presentations in the field for numerous venues including New York Times, Fortune Media, Dell Tech World and Lloyds of London Insurance. I am looking forward to this podcast

Ariel: It sounds like you have seen a little bit of everything related to cyber in your career! It's a tradition on this show for me to ask, did you always know that you wanted to go into computer science / cyber security? Was this your dream job when you were younger?

When I was growing up we did not talk about Cyber Security or even Computer Science. I really liked Math and Physics. Therefore, I wanted to study Math and Physics and be an educator in Math. However, when I went to college I started reading about computing and in grad school in England combined Math and Computer Science to do a PhD in Theoretical Computer Science. My work in cyber security today as a researcher, software developer and more importantly an educator is beyond my wildest dreams.

Ariel: What's your top cybersecurity tip for the general public?

Cyber-attacks are real. Therefore, you have to practice proper cyber hygiene. That means changing your passwords frequently and also backing up your files daily. You also need to ensure that you have installed anti-malware software and also the latest patches that vendors offer. Think of it as a virus (e.g., the novel coronavirus). To handle this virus, you have to make sure you are healthy and get the necessary vaccines. Just like the virus, malware (that is, the malicious software), planted by the hackers, can spread, and mutate. You need to take all the precautions to combat the problem.

Ariel: Throughout your career, you seem to have worked in many industries – commercial, federal, and academic – how do you see these industries working together to advance cybersecurity?

Over my 42 year career I have worked in the commercial industry, research lab, federal government, and academia. In academia, we focus on educating students. However, students also have to understand the real world problems and get practical training. This we can get from industry and government. Especially in cyber security, the government keeps track of the various attacks. Solutions to these attacks are usually developed by the industry. Therefore, it is critical that academia works with the government and industry to develop not only cutting edge solutions but anticipate what the future challenges we may face and address them.

Ariel: Your passion sounds like being a professor and training the next generation with your many journal articles, conference papers, books, and patents. Why is cybersecurity education important?

First, I believe that cyber-attacks are not going to stop. As we make progress with technologies (e.g., pacemakers, artificial intelligence (AI), power grid), the attacks will increase. Therefore, we need to have an educated workforce to solve the challenging problems we are going to face. Our students are our future. They will go on to have careers in academia, industry, and government. We need to equip them with the necessary skills to address the cyber security challenges. Many of those in my generation got their education in Math, Engineering and Computer Science. We did not teach cyber security say 30 or 40 years ago in most universities. Therefore, we had to learn about cyber security on the job. Our students will have an advantage as they will have the education when they start their careers. This in turn will enable them to better address the challenges.

Ariel: What's the most influential book you've read?

I have read many books over the years. I believe that education is lifelong. Sometimes I like to go back and re-read the basic books even in areas like Math. One book in Cyber Security I would say my favorite is Shon Harris' book on CISSP (Certified Information Systems Security Professional) All In One Exam Guide. It explains clearly what Cyber Security is about. Ms. Harris used to come up with a new edition every few years. Sadly, she passed away a few years ago. I hope the publisher will continue to publish new editions of this book.

Ariel: What does the cyber world look like in 5 years? How will quantum computing impact security?

When I think of 5 years from now, I get terrified. This is because we will continue to develop new technologies. This means more cyber-attacks. We are beginning to use say AI in every area from healthcare/medicine to finance manufacturing. Imagine if these AI systems are attacked. They would then produce incorrect results and that could cause chaos. Therefore, we need to develop AI systems that can handle attacks. While developing security solutions is critical we cannot forget about data privacy. Because of say AI, we can now mine and extract nuggets that could violate privacy. AI techniques can also be biased and discriminate against individuals. Therefore, we need to develop AI techniques that are secure, fair, unbased and ensure privacy.

Quantum computing is also a huge worry. First of all, quantum computing will do winders in handling say very large amounts of data and process the data rapidly. For example, quantum computing will be able to break the encryption code in milliseconds while the current high performance computers will take millions of years to break the code. Therefore, we will not have any security with quantum computing. As a result, cyber security researchers are developing techniques for what is called post quantum cryptography. It is hoped that with these techniques the encryption code cannot be broken by quantum computing.. So, we have a lot of work to do.

PART 2:

We’re back with part 2 with Dr. Bhavani, a professor of computer science at the University of Texas at Dallas and co-director of the centers for Women in Cyber Security and Women in Data Science. She focuses on cyber operations, diversity initiatives in cyber security, and data science. In this episode, we’re going to focus on the intersection of personal and technical elements, with a slight lean towards diversity and inclusivity.

Ariel: Why would you recommend cybersecurity as a career path to women and underrepresented groups?

I have given talks at various events for woman on “Why a Career in Cyber Security for a Woman.” Many of the key points I made also apply to the underrepresented communities. Here are some of the top 5 reasons I give. (i) Cyber Security is an intellectually exciting and challenging field with people from different fields such as computer science, risk management, and social science, working together. You get so much satisfaction when you are intellectually stimulated. (ii) Cyber Security solutions solve problems that occur due to cyber-attacks. This would in turn help people and businesses. This is very rewarding. (iii) There are many opportunities in cyber security and why not women and underrepresented minority communities take advantage of these opportunities. (iv) As long as we have technology cyber-attacks will continue to happen. Therefore, one can expect some level of job security. (v) Cyber Security is a high paying field. A high paying job is a must especially for a woman.

Ariel: What barriers do you see for women and underrepresented communities in the field of cybersecurity, and how can we mitigate these obstacles for them?

The barriers for women and underrepresented communities in cyber security are the numbers. Around 10 years ago the number of women in cyber security was around 10%. Now it is in the high teens. Also, for many areas in cyber security, especially say in systems security the numbers I would say are less than 10%. The numbers for underrepresented minority communities in cyber security are much lower. So, when there are so few women and underrepresented minorities in cyber security, it is difficult for them to get lucrative jobs. It is due to bias in general, often subconscious. People often tend to hire people like them. Furthermore, many of those in senior administration are men not from the underrepresented communities. As a result, the statistics are depressing for women and underrepresented communities. We need to motivate more women and those from the underrepresented communities to study cyber security. This has to start not just in college or high school but at a much earlier age. If we all do our part we can produce better results.

Ariel: If you could give a piece of advice to the next generation of cyber warriors, what would that be?

There is so much to tell them based on my experiences. First and foremost, cyber security is evolving rapidly. Therefore, you have to adapt to the changes and learn about the new types of attacks and the solution being developed. Learning is a lifelong process. Even after working for 42 years, I still try my best to spend at least an hour a day learning new material. This also expands the mind and thinking process. Second, you also have to get practical experience. That means understand patterns for various types of malware. Malware is usually just a piece of software. Therefore, learn about the tools that are used to detect malware and develop your own tools. Third, which I believe is most important, develop a passion for the field. Please don’t do it just because you get a good pay. Do it for the love of the subject.

Ariel: What is your hope for the future of the workforce and academia for cybersecurity?

My hope is that we can all work together to solve the challenging problems we are facing. This means diversity at multiple levels. First and foremost, we need more women and underrepresented minorities. We also need age diversity. While the younger people may be quick to learn new things, the older people come from vast experience in the field. They may know what works and what does not. We also need diversity with respect to technical areas such as computer scientists, computer engineers, mathematicians who specialize in risk and decision sciences, business specialists who work in cyber governance and auditing, social scientists who examine the societal impact including privacy, and psychologists who try and understand the mind of the hacker. We also need lawyers to advise us on legal aspects of cyber security and privacy. Finally, we need diversity with respect to academia, industry, and government. That means those in academia have to work with those in the commercial industry and government to understand the problems and develop practical solutions.

Ariel: How did you get into Cyber Security?

It was by chance. As soon as I finished my PhD in the UK we moved to the US in 1980 when I was 25 for better opportunities. My husband got a research scientist position at the Petroleum Research Center in Socorro New Mexico. I was offered a tenure track assistant professor position at New Mexico Tech. I turned down the offer as my son was a baby at that time. So, I took a visiting faculty position. The following year we moved to Minneapolis as my husband got a job at 3M. I continued to teach at the University of Minnesota for two years as visiting faculty. Then I wanted to get a more permanent job and joined Control Data Corporation (one of the top 3 computer companies at that time) and worked as a senior software developer. After just over two years and getting the product released, I wanted to get back into research. Then something wonderful happened. Honeywell had written a proposal to the US Air Force for a project on developing a secure database system. They were looking for a US citizen to work on the project back in1985. I became a US citizen that year, Honeywell won the contract, they interviewed me and hired me. All three events had to occur for me to get into cyber security. Since then, my career has been great. From Honeywell to MITRE, a federal research lab in Boston, and then to the National Science Foundation (federal government) in Washington DC and then academia as a tenured full professor at the University of Texas in Dallas. I was extremely fortunate to get that lucky break in 1985.