PROFILES IN **CONFIDENCE**

WOMEN WHO ARE LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

THERESA PAYTON

Former CIO, White House

"We are doing security wrong, and also doing it a disservice, because security should be an enabler through enhancing customer experience and revenue"

As the former CIO of the White House and with many years of experience, Theresa Payton is a recognized name in security, and a truly dynamic figure whose intelligence, passion, and drive permeate to all of those around her. With a hunger for identifying key cyber security solutions, Theresa has evolved into one of the most respected experts, and she embodies a true evangelist with her forward-thinking perspective.

Payton shares her thoughts on women in security, as well as key considerations for continuing to push the industry forward.

GEEK IS **CHIC**

Payton has only a small circle of close female friends who work on the technical side of security. "It is fabulous that more women are on the product, sales, and marketing side, but I would like to see more women in the analytical, technical, and ethical hacker side." This lack of female presence is in part due to the image problem security faces.

Payton mentions a Girl Scouts of America study that discusses how women have historically chosen careers where they have a connection and direct correlation to helping people. "Security has not done a good job of showing how cool it is to join the 'good fight' and protect friends, family, and corporations from the bad guys," says Payton. The industry has failed in demonstrating this exciting side of security, and the obvious correlation to helping

people is often lost. When Payton is evangelizing and recruiting people to join the industry, especially women, she tells them 'it's chic to be geek', and promotes the image of having a direct impact on customers. She believes that this will influence more women to seek out security-related professions and move the needle on elevating the attraction to security.

THE POWER OF **MENTORSHIPS**

Payton's mentor always told her that when you are the first female manager or first female on a project, be aware that people might be uncomfortable because it may be new to them. Payton says, "If you can disarm and charm them by asking if anything you are doing makes them uncomfortable, then you open up an honest dialogue that helps avoid issues later on." She emphasizes the importance of striving for open, authentic, and constructive dialogue in order to achieve collaborative success.

Payton believes that all women should seek out a mentor and do so with a clear notion of purpose and dedication. "You get out of it what you put into it and you should work hard to show your mentor that you are willing to put in a lot effort. Make sure your mentor understands that they will see a return on their investment and time. If you do this, is it hard for someone to turn you down, and you are going to see a lot out of that relationship," says Payton.

SECURITY AS A **BUSINESS STRATEGY**

In many organizations, executives view security as a compliance and risk exercise. "We are doing security wrong, and also doing it a disservice, because security should be an enabler through enhancing customer experience and revenue," she comments. The vital piece of strategy that many organizations lack is the impression that they are a technology company first. For example, banks are technology companies that do banking for a living and retail companies are technology companies that sell clothing and merchandise for a living.

While there is no one size fits all approach, Payton believes that the CISO and CIO should not be competing roles. "My hope is that over time, if you have hired the right CIO and CISO, then they do not have to report up to different places in the organization. They should not be competing roles, they should be complimentary," she says. This alignment, paired with a business-focused value strategy, is a recipe for success. By enabling the Board Room to understand that customer confidence and revenue are key competencies of security, many challenges of gaining budget and resources will dissolve.

For a CISO or security leader to attain this level of maturity, Payton recommends starting with great online resources and watching videos of how others solved complex security problems, such as TedTalks which present in terms of business value. She also believes in reading business periodicals that anyone on the Board would read and noting the words they use so you may speak their language and provide solutions that they easily understand. Payton says, "It is important to learn from luminaries in the industry who have cracked the code on how to speak 'tech and exec' at the same time, so when they hear from you, you receive the funding and resources you need."

Security AWARENESS CULTURE

Since 95% of breaches are due to human error and 78% by tricking the user, Payton recognizes that many awareness programs are proving ineffective.

"What companies need to do is take a step back and ask themselves which assets their employees, vendors, and contractors are touching. They need to ask if it would prove catastrophic if they made a mistake and 'bad guys' got in. It is important to recognize which one to four assets fall into this category and then focus an education and awareness program around these," says Payton. An example she provided was a healthcare organization that switched up training and focused on how employees could protect their elderly parent from internet fraudsters and children from reputation risk and internet predators. By tying corporate security goals back to lessons they were teaching, they experienced a large improvement in their post-training social engineering exercises and had better retention.