All interviews were conducted by DEBORAH FEYERICK

Deborah is an award-winning National Correspondent specializing in security, crime, terrorism and breaking news. Deborah was part of CNN’s team of anchors & reporters for 20 years.
Nashira Washington Layade is SVP, Chief Information Security Officer for Realogy Holdings Corp. The company elevated the CISO role to an SVP level when Layade arrived. Born in Brooklyn, she was convinced she would go to Harvard and become a divorce lawyer. With a strong aptitude in math and science, Nashira’s dad had other plans for her.

**D F:** Tell us a little bit about your background and what drove you into the tech industry.

**NASHIRA:**
My dad told me I was going to be an engineer. I went to a high school summer program at Massachusetts Institute of Technology (MIT) and studied tech and loved it, but I thought, “Okay, fine. I’ll be an engineer.” For college, I got into MIT, but much to my parents’ disappointment, chose University of Pennsylvania for the opportunity to combine both engineering and business classes at Wharton.

I majored in Computer Science and between my junior and senior year, I landed an internship at Telcordia Technologies and was offered a full-time job upon graduating. At Telcordia, I was first introduced to InfoSec, and I fell in love and never looked back. There, I was supposed to be a consultant and do assessments of banks, primarily in South America, but the company took a downturn.

After Telcordia, I went to The Windermere Group as a United States government contractor. I worked out of Fort Monmouth supporting the first Afghan war, Operation Enduring Freedom, doing intrusion detection and penetration testing to keep the systems safe there.

**D F:** The cyclical nature of government contract work and its financial uncertainty wasn’t something Nashira liked. And, she was ready to put down roots and buy a home. Just over a year after graduating, she was hired at Bloomberg LP.

**NASHIRA:**
I was 25 and worked third shift at Bloomberg, which was not so good for my social life. I worked 12-hour shifts, from 7 PM Saturday night to 7AM Wednesday morning. Because I had off Wednesday through Friday, I was able to get a master’s degree in Telecommunication Networks at Polytechnic University before it merged with New York University.

At Bloomberg, I worked in the data center monitoring their Intrusion Detection Systems. After 10 months, there was an opportunity on the corporate side to work directly for the CISO. They were looking for someone with 5 to 7 years’ experience. I had 3-years’ experience, but thought, ‘Heck I’ll let someone else tell me NO before I tell myself NO.’ I got hired. My boss was really amazing, taught me a lot and didn’t hold me back.

After working for Bloomberg for 3 years, I was ready for another challenge and wanted to learn more about the tech industry. Citibank hired me to do security analysis for mergers & acquisitions but then converted my role into conducting third-party vendor reviews. It was a massive organization, and I was able to move around the organization supporting both corporate as well as a revenue generating business unit.
F: With respect to changing jobs and taking on new challenges, what is your guiding principle?

NASHIRA: I do not fear change, and I don’t fear taking on new and challenging roles. I search for opportunities that allow me to expand both my knowledge and skill-base. One thing I’ve been very big on is stability because my mortgage has to be paid. After three and a half years at Citi, I went to Prudential Financial in Newark. This was at the time when HIPAA Hi-Tech and the Massachusetts data breach privacy law came out. My role was a 50-50 split between information security and data privacy. During that time, I got married, pregnant and took some time off to deal with a family emergency.

By this time, I’d been in the field for 16 years building my career to be a CISO. When Time Warner’s first CISO role posted, I didn’t apply because of the decentralized nature of the organization. If something were to impact any of the TW divisions, it may have impacted the entire company and impacted the stock price. It was too risky operating in a decentralized organization, and the CISO has the ultimate responsibility for cyber risk across the enterprise. I knew I wanted to be a CISO, but the Time Warner model didn’t work for me. The opportunity at Realogy came along and it offered a chance to build — I love to build.

F: In 2011, Nashira was hired at Time Warner, which was developing and maturing its corporate security program.

NASHIRA: Similar to when I was at Bloomberg, Time Warner was another acceleration point for my career. Before I joined the company, they didn’t have a data privacy program in place. I ran the corporate information security, data privacy and information risk management program for nearly five years.

By this time, I’d been in the field for 16 years building my career to be a CISO. When Time Warner’s first CISO role posted, I didn’t apply because of the decentralized nature of the organization. If something were to impact any of the TW divisions, it may have impacted the entire company and impacted the stock price. It was too risky operating in a decentralized organization, and the CISO has the ultimate responsibility for cyber risk across the enterprise. I knew I wanted to be a CISO, but the Time Warner model didn’t work for me. The opportunity at Realogy came along and it offered a chance to build — I love to build.

F: You’ve had significant roles and 5 major organizations since graduating college. What lessons did you learn at each organization?

NASHIRA: Bloomberg, Global Head, Sept 2002 - Nov 2005: Allow other people to say ‘no’. But don’t say ‘no’ to yourself. I only had 3 years’ experience in the field, not the minimum five years’ experience required in the job posting. My boss liked me, saw something in me, and hired me. Just go for it.

Citibank, VP Senior Risk Control Officer, Nov 2005- March 2009: Don’t be afraid to move around. The great thing about being in an organization with 300,000 employees is you can discover different parts of the organization. For me, the big thing was moving from a corporate position to working in a business unit, so I could fully understand the complaints, and how to resolve them.

Prudential Financial, Director InfoSec, March 2009 - January 2011: Prudential was all about the data security. It was the first time I had a reporting line into women. Prior to this role, I worked mostly for and with men. By comparison it was such an emotionally toxic environment. I learned how to be mindful of managing. That experience made me a kick ass manager and taught me how women sometimes overcompensate due to the different way we are often judged in Corporate America.

Realogy, SVP Chief Information Security Officer: Compared to the other organizations for which I’ve worked, it’s unregulated. That’s one of the reasons I love it. I can be a little more creative. I’ve been able to transform the security program — now it’s more risk-based. Here, I can build and, as I mentioned earlier, I get excited about building.

F: How do you develop women in the organization?

NASHIRA: I have a team of 33. Five of them are women who are responsible for the information security and privacy of 12,000 employees and 55,000+ agents. We have to kick ass. This year we became a sponsor of the Executive Women’s Forum. I am very vocal with both my team and HR about my interest in hiring from a diverse candidate base, with a specific emphasis on women. I’m all about encouraging women, supporting them, and pushing them to reach their maximum potential (and beyond). I send the women on my team articles, industry events, and anything of interest that will build them up and motivate them. I talk to them. Really talk to them and ask where they want to be and how I can help make the next best move for their career. I’m also aware of how men interact. I grab pizza, beers, and talk football. Just because I’m a woman, doesn’t mean I can’t be one of the boys as well. My office is a revolving door.

F: What about equal pay?

NASHIRA: When I first started at Realogy, I conducted a salary evaluation to self-educate. I also talk to my staff about market reference range & other concepts to help them understand their market worth.

F: Have you always been able to have so-called life/work balance?

NASHIRA: Part of my rationale for leaving Time Warner was that my work/life balance started to get crazy. When I first started there, I worked from home once a week. Unfortunately, there were changes in management that did not support remote-work and other types of flexibility that I relied upon. That’s not what I signed up for.

My priority is my son. He is first. Period. Point blank. I often tell my husband that if I die first, there are only three paragraphs to summarize my life and that he should not waste any letters, words, sentences, paragraphs about what I accomplished professionally. I love my career but being a CISO does not define me. It’s what I do, not who I am. My husband knows to use my three paragraphs to describe who I was as a Wife, a Mom, and a Christian and talk about how I helped my community.

I was blessed that my mom was a teacher. I had her around during summers. During the summer, my son stays with my parents in Georgia because I’m working. I bust my behind to give him a good life. I believe fundamentally that parents are minimally responsible to provide as good a life as their parents provided for them. My parents sacrificed A LOT to send me to schools like Andover and the University of Pennsylvania while supporting all my extracurricular activities (piano, viola, gymnastics, swimming, etc.).
D: Is it ever too early to start building a foundation for success?

NASHIRA: Not at all. My son is exasperated at how much I push math and science on him, but it’s the way I was raised. My parents consistently pushed me to always be a top student. I once got a 92 percent on a test and my father said ‘Baby, you can do better. You can get a 100.” The next test I made the 100 and his response was “Oh, this is good baby, but did you ask for extra credit?” I was only in the fourth or fifth grade at the time. Because of that foundation, I constantly push myself and those around me. There is no such thing as “good enough” or resting on laurels. I always ask myself ‘What’s next? What’s next to achieve and conquer, Nashira?’ I do realize that at some point I have to slow down. I am sometimes afraid that I’ll get to 59, retire, and my brain will conk out from over-exhaustion from being constantly pushed. It won’t know how to rest and relax.

D: If you were to meet the most interesting person in the world, what is it you would want them to know about you?

NASHIRA: That staying grounded matters. My family is everything, and I’ve been blessed beyond belief. My parents have been amazing. They worked their tails off to get me where I am. Considering where I grew up, statistically speaking, I’m not supposed to be where I am. It’s important to remember from where you came and to give back.

D: You describe the company mission at Realogy: “We do real-estate and holistic management of real-estate.” What worries you most as CISO? ?

NASHIRA: It’s really interesting to partner with independent agents, many in the 50-60 age range, who are responsible for the largest transaction of a person’s life. They’re not employees, and I cannot control their devices. Reputational risk is huge. If something major were to happen to one of our brands, it can present a major risk to our company. This is what keeps me up at night.

D: Do you still have a “love affair” with InfoSec?

NASHIRA: Yes. I felt the same way when I was first introduced to the field. I’ve been blessed to reach this stage of my career before the age of 40. I plan to retire at age 59. So, 20 years to go! I’m grappling with what’s next. I’m flirting with law school and am figuring out how to bridge that with my security experience. I did what my dad wanted me to do in pursuing the engineering, but I am a big supporter of having underrepresented minorities pursue careers in math and science.
As Senior Vice President and Director of Security and Fraud Operations at PNC Bank, Susan Koski manages a team of 430 cyber and fraud professionals. She is driven by curiosity and a constant need to learn. “In cybersecurity,” she says, “You never have the same day twice.” Now juggling the demands of motherhood, Koski shares some of the lessons she has learned along the way.

**DF: How did you get interested in cybersecurity?**

**SUSAN:**

I always had an aptitude for math and analytical subjects. My senior year in college, I was exploring what I wanted to study. My mom and dad never told me there were limits. It was always, “Go do what you want.” I did think about law school but decided to pursue engineering as it fed my propensity for math and analytics. I received my electrical engineering degree from the University of Pittsburgh and spent the first part of my career in application development for nuclear control systems, performing software testing, validation, as well as coding.

During this time, I attended night school at Duquesne University, which had a great program for students who were also working full time. I received a Master of Business Administration (MBA) and took a job with a smaller firm, which fed my creative mindset. The company culture was similar to a start-up, and while I enjoyed it, I was searching for more. I attended a job fair and received two offers, taking a position with Mellon Financial in Pittsburgh in their information security department. It was my first job in information security, in an area I knew the least about.

**DF: Tell me about that job at Mellon and its subsequent merger with Bank of New York.**

**SUSAN:**

I was at Mellon Financial of Pittsburgh from 1998 to 2006 leading the Network and Perimeter Defense function. Here, I managed defensive operations, vulnerability management, digital forensics and network assessments. When the company merged with Bank of New York, I was brought in to work with senior leadership to merge the Technology Risk and Information Security functions. In that role, I learned about mergers of equals and the key methods to a larger integration, having worked on many mergers and divestitures previously.
**DF:** How did you look for your next job?

**SUSAN:**
Through my network, I began exploring opportunities for a larger role. A colleague on the Board of Directors at Synovus, a regional bank, indicated they were seeking a Chief Information Security Officer (CISO). She introduced me to the person who would be my new boss. Without that connection, I never would have had the opportunity.

As I was interviewed, the Chief Operating Officer and his staff really impressed me. The initial offer wasn’t enough to make the move to another state. However, I knew that taking this role would allow me to work with a leader with visionary skills about customer experience in banking, as well as take the next step to the C-Suite.

**DF:** What do you consider one of your biggest successes there?

**SUSAN:**
My biggest success was building an excellent team that worked incredibly well together. We were a lean, mean fighting machine with incredible collaboration and comradery. I’m still connected to them.

**DF:** What is it that excites you about cybersecurity?

**SUSAN:**
What I love about the field is the continual learning opportunities. I always ask myself, “How do I feed my curiosity?” That’s a large part of how I got where I am. In cybersecurity, you never have the same day twice, which is perfect for someone who doesn’t like to do the same thing over and over. Also, in cybersecurity, you have to question why and have the ability to consider various hypotheses, manage relationships, negotiate and influence for appropriate risk management.

**DF:** The merger challenged you, not only to balance both responsibilities, but it also helped you segue into risk management.

**SUSAN:**
It allowed me to learn something new. I pulled together all the data and analyzed how to combine it for maximum efficiency and then presented it at an executive level. Technologists tend to be detailed-oriented but that’s not how to communicate to management. This role helped me hone executive management presentation skills. From there, I was asked to take a more significant role in the firm, managing technology risk assessments globally. The focus was looking at risk but through a technology lens: infrastructure, applications, user-defined technologies and third parties. For me, it was something else to learn, much broader with a global lens, including regulations. After about four years, I decided it was time to search for opportunities outside of the firm.

**DF:** Did you turn down the job or negotiate for a better position?

**SUSAN:**
I called a good friend and told her about the offer. She said, “Did you ask for more? You need to ask.” I called and asked for an increase and hadn’t even finished my sentence before the increase was approved. As women, we don’t ask. We think if we put our heads down, someone will notice, someone will give us the opportunity. You have to have the skills, but you also have to ask—for the project, for the opportunity, for the raise.

**DF:** Did you regret not asking for more?

**SUSAN:**
At first, I realized that I possibly could have received more, but what I took away from this was much more important—to ask. After being there six months, my boss rewarded me. He handed me a piece of paper and said, “You just got a raise. You’ve done such a great job, we’re recognizing you for that.”
Facebook COO Sheryl Sandberg refers to the Tiara Syndrome. Women are taught to keep their head down, work really hard and then someone will recognize it and place a crown on their head. Essentially, we’re told to wait for power to be offered rather than seize it.

SUSAN:
I think you are spot on. As ladies we need to think about our marketability and our worth. I rarely see ladies come into the market who know exactly what they are worth. Men know all the time. Women have to better understand what the market is bearing.

For all jobs, I do my research. I talk to friends who are recruiters to identify the industry benchmarks. Those confidants provide input such as, “Don’t take another job unless you get X percent more.”

The other key piece is networking. I spend time getting out in the community, going to security meetings, showing people what I can do. This provides a family of people if I need advice on the job market and the industry, which is incredibly valuable.

What was your biggest challenge at the company and how did you want to make an impact?

SUSAN:
Short answer - rebranding and becoming a trusted advisor. As Chief Information Security Officer, I was in charge of everything in cybersecurity: policy, governance, financials, architecture, engineering, response, vulnerability management, application security, regulatory compliance and business continuity. In this role, I was able to build the functions from inception.

I went through financials, and we found things we were paying for that we weren’t using. My thinking was, “How can we be creative in what we do with these funds in a TARP-funded bank?” The other challenge we had was that people thought of us as the mystery team that did secret things and always said, “No.” You want the business to view the team as a trusted advisor to deliver in a safe and secure manner and to be able to say, “Yes, with the right operating conditions.”

Second, I rebranded my team. Rather than Information Security and Business Continuity, we modified the team name to Information Risk and Resiliency. This rebranding was the first step in changing the perception of the team and initiating the path to becoming a trusted advisor. For the first year and a half, the team name to Information Risk and Resiliency. This rebranding was the first step in changing the perception of the team and initiating the path to becoming a trusted advisor. For the first year and a half, we had was that people thought of us as the mystery team that did secret things and always said, “No.” You want the business to view the team as a trusted advisor to deliver in a safe and secure manner and to be able to say, “Yes, with the right operating conditions.”

For the first year and a half, we had was that people thought of us as the mystery team that did secret things and always said, “No.” You want the business to view the team as a trusted advisor to deliver in a safe and secure manner and to be able to say, “Yes, with the right operating conditions.”

For the first year and a half, we had was that people thought of us as the mystery team that did secret things and always said, “No.” You want the business to view the team as a trusted advisor to deliver in a safe and secure manner and to be able to say, “Yes, with the right operating conditions.”

SUSAN:
In a career of almost thirty years, I have had incredibly supportive male leaders. At Mellon, a gentleman in a career of almost thirty years, I have had incredibly supportive male leaders. At Mellon, a gentleman was hired who brought a whole different professionalism and learning opportunities. He coached me on the culture of the company and how to present myself to showcase what I could bring to the organization. Men are often very supportive of women. If there were undertones of lack of support, I never let that stop me. If you’re going to be a blocker, I’ll find an enabler.

In a career of almost thirty years, I have had incredibly supportive male leaders. At Mellon, a gentleman in a career of almost thirty years, I have had incredibly supportive male leaders. At Mellon, a gentleman was hired who brought a whole different professionalism and learning opportunities. He coached me on the culture of the company and how to present myself to showcase what I could bring to the organization. Men are often very supportive of women. If there were undertones of lack of support, I never let that stop me. If you’re going to be a blocker, I’ll find an enabler.

Story Behind the Story: Interview with Susan Koski

F: Why you?
SUSAN:
My theory and wealth of knowledge. We always have to be prepared for our adversaries’ next move, and I look at that in a couple of different ways. starting with executing new things we need to do. Talent management is also a passion, and I have a knack for bringing teams together and inspiring them to achieve their potential. My philosophy is: Make sure we are doing the basics really well, make smart investments, focus on our talent and allow our talent to innovate.

F: You’re now Senior Vice President and Director of Security Operations at PNC. What are the challenges?
SUSAN:
My team is about 430 people, covering both cybersecurity and fraud. Having the fraud background was a key driver for attaining this role as PNC has aligned cyber, fraud and physical. The key opportunity is fully converging the functions and fusing key capabilities in fraud and cyber. beyond just a reporting structure, creating something new and exciting. We have completed this within Intelligence. Incident Management and Insider Threat.

F: What role did women play, positive or negative, throughout your career?
SUSAN:
In my journey, there aren’t a lot of ladies. A good friend of mine grew up in technology and security roles. twenty years ahead of me, and her lifelong learnings have played a pivotal role as a coach, mentor, friend, and someone I call for counsel. Second, the lady on the board of directors who introduced me to this new opportunity. These ladies are inspirational game-changers and leaders.

We ladies are not always supportive of one another but we need to be. Some won’t support you because they don’t want you to get ahead of them, and I experienced that once in my career. At the time, I asked if I could make a difference in that organization. Despite years of trying, I determined I had to leave that organization.

The positive experiences, however, outweigh the negative. My boss at PNC is exceptional at assessing information and guiding teams to follow a logical path. She will hold you accountable, but she also lets you try things. Often, we learn more from the things that don’t go well, compared to the things that do go well.

F: What about the men you have worked with?
SUSAN:
In a career of almost thirty years, I have had incredibly supportive male leaders. At Mellon, a gentleman in a career of almost thirty years, I have had incredibly supportive male leaders. At Mellon, a gentleman was hired who brought a whole different professionalism and learning opportunities. He coached me on the culture of the company and how to present myself to showcase what I could bring to the organization. Men are often very supportive of women. If there were undertones of lack of support, I never let that stop me. If you’re going to be a blocker, I’ll find an enabler.

In a career of almost thirty years, I have had incredibly supportive male leaders. At Mellon, a gentleman in a career of almost thirty years, I have had incredibly supportive male leaders. At Mellon, a gentleman was hired who brought a whole different professionalism and learning opportunities. He coached me on the culture of the company and how to present myself to showcase what I could bring to the organization. Men are often very supportive of women. If there were undertones of lack of support, I never let that stop me. If you’re going to be a blocker, I’ll find an enabler.

F: What was your biggest challenge at the company and how did you want to make an impact?
SUSAN:
My team is about 430 people, covering both cybersecurity and fraud. Having the fraud background was a key driver for attaining this role as PNC has aligned cyber, fraud and physical. The key opportunity is fully converging the functions and fusing key capabilities in fraud and cyber. beyond just a reporting structure, creating something new and exciting. We have completed this within Intelligence. Incident Management and Insider Threat.

SUSAN:
Often, we learn more from the things that don’t go well, compared to the things that do go well.

In a career of almost thirty years, I have had incredibly supportive male leaders. At Mellon, a gentleman in a career of almost thirty years, I have had incredibly supportive male leaders. At Mellon, a gentleman was hired who brought a whole different professionalism and learning opportunities. He coached me on the culture of the company and how to present myself to showcase what I could bring to the organization. Men are often very supportive of women. If there were undertones of lack of support, I never let that stop me. If you’re going to be a blocker, I’ll find an enabler.
DF: Cybersecurity, how have you seen it evolve since you got into the field?

SUSAN: Where we all started, it’s identifying patterns and assessing behavior. It’s how do we defend against it and how does the adversary change? I’m looking for indicators in the digital space—an application that is not acting right. It’s very pattern-oriented. Adversaries figure that out. Where we have evolved as an industry: My information is out there. Yours is out there. So, who is trying to use your credit? It now has to evolve past password and similar binary information.

Our experience is how I intersect with technology and what I do with that: behavioral risk. With someone who might inbox inside a network, all of a sudden, they are trying to access something they’ve never done before; their behavior changes. As adversaries evolve, like a cat and mouse game, everything will be behavioral. How do I know who you are? Do I know how Susan types or Susan’s actions on our mobile website? Because of the behavior, I have a higher degree of confidence that it’s Susan. Data science and pattern analysis are more at the forefront of cybersecurity.

DF: You have now expanded your role to “New Mother.” How does that impact what you do?

SUSAN: It changes you so much. Until you are a mother, you don’t know the joys and the priority focus. It has made me much more conscious of my time. I have 430 people working for me, and I can delegate and enable their learning potential with meetings and opportunities. I’m much more selective on the meetings that I attend, focusing on the value add. I have great balance, a great husband, and a great nanny. It is about time management. Having a child requires you to be more selective about how you spend the time you have.

DF: What is your overall advice to women?

SUSAN: A-S-K. N-E-T-W-O-R-K. It is acceptable to ask for what you want. Take your power and change the situation or the story.

DID YOU KNOW?

Woman make up over half the workforce. However, woman make up less than 20% of U.S. tech jobs.
Quiessence Phillips built a career in cybersecurity by first taking things apart. In her role as Deputy CISO, Threat Management for NYC Cyber Command, she has helped unify the city’s once decentralized cybersecurity network to safeguard its IT systems and protect vital services. Phillips has risen quickly in a predominantly male-dominated field and learned how to manage in what she calls its “bromance” culture. “Words matter,” she says. “When you use the word ‘female,’ it almost loses its edge. Why can’t I just be a boss? Not a female boss. A boss.”

D: Did you think you were going to go into cyber?

QUIESSENCE: Yes, I always wanted to be in technology. I had a knack for reverse engineering things. I’m still the same way, taking apart things to see how they work, such as my parents’ VCR, my computer. In the realm of code, it’s the same. Something is engineered, and you want to reverse engineer to see how it’s created.

D: Who in your life influenced you most?

QUIESSENCE: My mother understood what I was good at. My mother is a connector. She knew she didn’t know it all, but she knew how to connect me with people who could give me knowledge and help me make the best decisions.

She was working at a bank and met a girl with a computer science degree. My mother told me, “You should meet this young lady. She is doing what you would be good at.” The girl came to my home, and I started doing research into computer science. I gravitated towards computing. I knew the power of what this could do, and if I understood at a deeper level, what it meant to me in my life.

D: What had the greatest impact on you during college?

QUIESSENCE: I joined the computer lab and worked for the network administrator, setting up all the network connections. I took everything they threw at me. I was interested in how effectively all the computers worked together, how we could make them more efficient with software, etc.

My bosses gave me tons of projects and allowed me to screw up a lot of things. The ability to play and test in a lot of environments with regard to computers and networks helped me understand the work, not only from a theoretical standpoint, but also from a practical one. I was studying coding languages, algorithms, etc. By the time I graduated, I had amassed a lot of network admin experience. I’m the first one in my family to graduate from college.
F: What has changed in the relatively short time you have been in cybersecurity?

QUIESSENCE: We're doing the same thing now that we were doing ten years ago. I took a lot for granted at the Federal Reserve that people are now just adding. There's more spotlight on the industry. There wasn't a lot of news about the threats we were facing at the time. A lot of the foundational work is the same. Now we have added components such as cloud computing, amassing so much more data because of the inter-connected devices, etc. At its foundation, the work is the same.

F: What do you see as the biggest challenges in cyber?

QUIESSENCE: There's so much data and only finite resources. That is and was one of the biggest challenges. That's where you have a lot of need for automation and orchestration. We know we are under-resourced. We have a lot of doors to protect and only finite resources.

F: What about on a personal level?

QUIESSENCE: There's a lot of bromance culture. It's a male-dominated field. It wasn't a huge issue for me, but not all women feel comfortable in that environment. At times, you have to have a thick skin; things men do or say in these environments may not have malicious intent but may have some negative impact on their female counterparts. Everyone has inherent biases.

F: You went on maternity leave while at the Federal Reserve. How did that affect you?

QUIESSENCE: I was twenty-five years old and gone for about six months to take time to focus on myself and my child. QUIESSENCE: However, times are changing and I think both parents want a healthy lifestyle for their child (or children) that allows parents to be more involved.

F: You continued to get promoted.

QUIESSENCE: I've moved up pretty swiftly based on my track record. I treat everyone the same. I'm fairly young in this industry. I did get some backlash, especially from older men who were my seniors before I became their boss. They weren't very happy with it. That was challenging for me being a leader. It takes time to understand the environment and why people feel certain ways. I did second-guess whether I was ready to lead a team of that size. At the end of the day, you get over that. You are awarded this job because of skill.

F: How did you overcome those feelings?

QUIESSENCE: Women have to get out of our own way. We undersell our abilities. If there's one job and ten responsibilities, a woman will say, "I can only do seven of ten." Whereas a man may only be able to do five out of ten but will say, "I'll learn on the job." It's one reason more women aren't applying for top jobs in cyber. Women tend to look at things we cannot do and say, "We are not enough." That mentality is flawed.

F: What about mentors?

QUIESSENCE: All the bosses I had that were men were incredible. I've heard horror stories from other women. Thankfully, I haven't had those experiences. My bosses have been super allies for me. I had one female boss, and she was awesome. She taught me a lot about how to carry yourself as a female leader.

F: What are a few of the lessons your female boss taught you?

QUIESSENCE: Women have to get out of our own way. We undersell our abilities. We undersell our abilities. Women have to get out of our own way. We undersell our abilities. Women have to get out of our own way. We undersell our abilities.

QUIESSENCE: Be financially strategic: I was going to leave the Federal Reserve and take a consulting job with a Fortune 500 company but decided not to. I'm very much into finance. I made good investments. I had been at the Fed for about four years. I was 80% vested. If I left, I would lose my vesting. My manager said, "One, this has nothing to do with career growth, but if you take this new job, I feel you will not be happy. Two, you are going to lose a lot of money if you leave before being fully vested. How much are they willing to pay you?"
**D:** Tell me how your boss counter-offered, giving you both a promotion and lifelong financial advice.

**QUIESSENCE:**
She asked me, “Is it about the money or the work?” For me it was both. I felt I needed a change. I needed to shake things up. My boss said, “We can give you a different type of work, and in this instance, you can fulfill both needs, and you don’t lose vesting. Resist the urge to leave now. Next year you will be in a better position.”

I really appreciated that type of information. She didn’t have to share that with me. It made me reconsider certain choices and affected how I make decisions. I decided to stay, and I carry it forward. I always want people to make the best decision for themselves, and they have to be happy with the decisions they make. Don’t settle with short-term fixes.

**D:** What are the top three things you bring as a woman in cyber?

**QUIESSENCE:**
**Perspective:** I bring a different perspective to the table. I feel diversity is important because of the unique opinions and perspectives people bring because of their own upbringing. Think about emojis. There were no black emojis until 2015. If there were more diverse groups making decisions that affect a wide range of people, different decisions would be made. Also, words matter. When you use the word “female,” it almost loses its edge. Why can’t I just be a boss? Not a female boss. A boss.

**Inspiration:** I assume other people know what I know. My mother used to say, “Just because you know it, doesn’t mean others do.” As I began to break out of my shell, I got an overwhelming response from other women. “You inspired me to go to school for this, pursue a career in technology, in cyber,” both men and women. I would get so many different messages about the impact on their lives and how I made them think differently or forge into areas they wanted to pursue.

**Mission-driven:** I am blunt. I am mission-driven. I like to cut out the fluff and focus on mission. While the work is important, the journey is just as important. We want to make sure we're having fun, making progress, and setting the stage for people coming behind us.

**D:** Mentoring is a big part of your life. You created the non-profit JOURNi.

**QUIESSENCE:**
My co-founders and I met at an event teaching kids to code and exposing them to different areas of technology. We wanted to bring a program to Detroit, specifically to educate and create exposure for the under-served demographic. I’m the first in my family to graduate from college. If you have two parents in your household and they are both engineers, you will likely be an engineer. Exposure is key.

We’re teaching entrepreneurship, programming and other foundational elements that add to success, and everyone is eating it up. But there are fundamental issues that create challenges our communities don’t necessarily face. Instead of starting with technology fundamentals, we had to start with accessibility and transportation. There are students who are incredibly smart, dedicated and willing to do this work, but are unable to get to a learning center from one side of Detroit to the other because they have no bus money.

**D:** How did you grow at each job to take on the responsibilities you have now?

**QUIESSENCE:**
In each of my jobs, I’ve developed different sets of skills and different ways of thinking about risk management and working effectively. I’ll learn on the job. It’s one reason more women aren’t applying for top jobs in cyber.

Federal Reserve, July 2007-January 2013, Operations Supervisor & InfoSec Analyst, National Incident Response Team: I amassed knowledge and discipline, monitoring threats, incident response, managing a 24/7 operation. I got my feet wet in all areas.

LookingGlass Cyber Solutions, LLC, January 2013-September 2013: I worked for several financial institutions dealing with client relations, understanding different environments, providing cyber threat intelligence, third-party oversight, etc. There’s so much data available to be consumed. But proper use cases for the data, identifying logging requirements are important pieces prior to ingestion. Let alone analysis.

Barclays, VP Cyber Security Operations, Incident Response, Sept 2013-Oct 2017: At Barclays, I worked with colleagues in different parts of the world. This provided an interesting perspective, not only from a cultural optic, but also from a regulatory one.

City of New York, Deputy CISO, Threat Management, October 2017-Present: Coming to the City of New York opened my eyes. I look at everything differently. I appreciate the work that goes into running a city, especially one as large and dynamic as NYC. When we’re investigating a cyber event, we’re not just thinking about the technology, the money that could be lost, or the brand reputation, the most important thing is the potential impact it could have on the people who live here. Think about the services the city provides like clean drinking water or automated benefit checks to underprivileged parents. If those systems are tampered with, the outcomes can be life-impacting.

**D:** What is your biggest achievement personally and professionally?

**QUIESSENCE:**
I never really look at it like the “biggest achievement.” I do a lot of small things that add up to something great. Although I live in a ‘response’ kind of world, I focus a lot of time on preventative work. If you don’t prevent, then you will be stuck in a cycle of responding to the same events.

The biggest achievement from a leadership perspective is to help people see and be the best versions of themselves. It is rewarding to help others achieve their goals while we make strides together to achieve the mission.

Personally, and within this industry, I would say my Securing-Your-Path initiative is pretty important. I’ve been able to touch women who are interested in the field and ‘secure their path’ and make it a little bit easier for women coming after me. I’d like to see more women in the field. Those are my biggest achievements, besides my son!
Patricia Titus has held many interesting jobs. She began her career stationed in Japan as a morse code operator for the United States Air Force; moved on to the U.S. State Department; raised a family while working in Saudi Arabia, Germany, and Africa; and was the first person named CISO of a federal agency, a title she has held at several Fortune 500 companies.

F: When Markel approached you, you had left corporate America and were consulting for the Ponemon Institute, a research center dedicated to privacy, data protection and information security policy. What was it about Markel that pulled you back into the corporate world?

PATRICIA: I wasn’t sure I wanted to keep being a CISO. The head of Markel’s IT governance at the time had been given my name as a possible candidate for the CISO role. During our first conversation, she and I talked for a few hours and really connected. I always ask one question when interviewing: “Are you checking a compliance box?” The answer matters because it’s a gauge for how committed the company will be to security and with regulatory law pressing companies to hire CISOs. It can be a check-the-box exercise. Markel’s answer was honest. “Yes, we are checking a box, but it’s a very small one.”

Markel was committed to finding a cyber-security expert who could build a program not just for compliance reasons, but to meaningfully enhance their security program. And, they were willing to commit the assets and visibility necessary to do the job. I found that intriguing.

F: What factors did you weigh in making your decision to go to Markel?

PATRICIA: Markel’s culture and commitment were the key factors. The environment at my previous job was not very good, and I had left with my self-esteem and confidence shaken. I found the environment at Markel to be completely the opposite. Everyone I met during the interview process was so genuine. To the point I thought, this is too good to be true. Leaders actually wanted to do what’s right for the company — no airs, no political agenda — and they were genuinely looking for someone to come in and rebuild the entire program.
I have a 100-day plan and a methodology I have developed over many years, which I use to assess a new organization.

First thing is to look at human resources and conduct a workforce assessment. I have found there are three types of people working in security. First are those who are skeptical or cautiously optimistic about a new CISO. They don’t understand your operating model and worry about how they will fit into the new regime. The second type are those individuals who are long-standing employees and have significant loyalty to the company. A new CISO must objectively assess if they have the right critical thinking skills to move the security organization along and, if not, what training will they need. Third types are the flight risks. Their resumes are ready to go and they have the potential to walk out the door. With retention in cyber security being what it is, not everyone is willing to say a breach is likely. That’s pretty honest.

My motto is, “Just enough. Just in time. It doesn’t mean you won’t have a breach or a disruption, but are you practicing what to do when there is a problem? How do you identify it? How do you respond? How do you contain? It’s prevent, detect, respond and recover.”
F: On 9/11 you were working for the U.S. Treasury Department as a technical advisor to the CIO. When the planes hit the buildings, one of your first responsibilities was getting secure wireless communications to the crisis management teams. The work you did during the terror attacks clearly influenced your thinking and how you do what you do now.

PATRICIA: It was a defining moment that shaped many people’s lives. It goes back to the Girl Scout motto, “Be prepared.” I’m still a Girl Scout, and I believe its many defining moments in my life and career that have developed me into the well-rounded leader you see today. My defining moments included living in Saudi Arabia during the Mecca/Medina massacre; living in Africa at the peak of the AIDS epidemic; living through 9/11 near everything that was happening and having to execute plans. All those pieces and parts helped define my style of leadership today.

F: You took what you learned during 9/11, built out another secure wireless communications platform for the 2002 Winter Olympics in Utah, and then went on to play a vital role creating a brand-new government agency, the Transportation Security Administration.

PATRICIA: TSA was the pinnacle of my career. I was part of the early start-up team, which I liken to an organization of patriots. We had left the security of our jobs to be on the ground floor of a brand-new federal organization. In the TSA environment after the 9/11 attacks, we were so driven and focused on our mission to secure the traveling public. It was just amazing.

F: By the end of 2002, eight months after you joined, the organization mushroomed from a few hundred people to about 56,000 employees. Your rise was pretty steep, ultimately taking over all of TSA’s information security.

PATRICIA: I was the first person to be given the CISO title in the federal government. I started as the wireless program manager securing communications for federal officials at airports across the country. Next, I became the security manager. I kept asking my CIO to make me CISO, which he did. If I hadn’t kept asking, I would not have been given the official title.

There is a flip side however, which is be careful what you ask for. Being the CISO at the TSA, I didn’t realize how powerful the position really was until the day my CIO said, “Stop using security as a weapon.” Security is extremely powerful in a company, so use your power wisely.

F: Clarify what you mean when you say, “Security was a weapon.”

PATRICIA: As CISO I had been given the power to stop programs from moving forward based on risk assessments. These programs and applications were needed to advance our mission. And, of course, I wanted it as secure as we could make it and fully hardened. I wanted it all to be perfect and if it wasn’t perfect, I wouldn’t sign off on it going live. Because we were a new organization, I wanted zero risk. I realized as the expert, I had the power to say, “Don’t do it,” and they wouldn’t.

Yet, think of the consequences for not deploying capabilities. The US experienced planes flying into buildings, and I had to learn to operate my security program based on risk management and risk appetite. It’s not just a zero-sum game, and this is a lesson I have carried with me throughout my career. Use the power of authority to manage risk and help the company understand the level of risk they are taking.

F: Are you now more comfortable making decisions when you’re only 90% certain?

PATRICIA: It’s more like the 80/20 rule. 20% of your activities will account for 80% of your results. For example, we lived through Y2K. (The Millennium bug. Leading up to 12:00 AM, January 1, 2000, governments around the world launched a massive effort to implement new software, fearful older systems would not properly process ’00 digits, thereby resulting in a global meltdown). The things we thought were going to happen never did. Did they not happen because we planned so well, or because they weren’t going to happen anyhow? It’s the 80/20 rule.

Companies need a good risk-management strategy and a way to tier the criticality of their data based on its value. Not having this strategy could mean they’re investing too much or too little in protection capabilities. I’ve seen many CISOs get to a new company and go like gangbusters and before you know it, they get fired because the company can’t handle the cyber-fatigue. With security, you must find that delicate balance of “just enough, just in time” security.

F: How has your leadership style evolved over time?

PATRICIA: I had a career/life changing moment on how I lead people, after the US government sent me to the Center for Creative Leadership. Leaders need mentoring and training. I believe most people don’t ask for help enough, and especially women don’t ask for it, because they’re afraid they may be viewed as being weak or less skilled. But if you don’t ask for help, then those weaknesses become ingrained and your career can be derailed.
**DF: How did it change?**

**PATRICIA:**
My move to the top was pretty quick. Once I got into the executive ranks, I was a little bit full of myself, to be frank. I felt I had to be a man to do a man’s job. I honestly lost touch with my identity and was neither self-aware nor particularly humble. I was the person who would bring a group into the room and chew them all out. Maybe they needed it, but there are better ways to achieve success, as I learned. I thought I had to redo everybody’s work because I wanted perfection and thought it wasn’t good enough for me to put my name on it. I was stressed out, close to burnout, making myself ill, and making others around me unhappy.

The Center for Creative Leadership was yet another defining moment. I learned you can’t control everyone around you. The only person you can control is yourself. I had to relearn how to be self-aware, to realize I was not treating people fairly. I had convinced myself that everyone else was the problem. I had stepped so far out of myself. I had to find my way back and learn to be a good leader.

**DF: You say you felt you “had to be a man to do a man’s job,” when the more accurate description should be this is a job and I’m the most capable person to do it. Did you have a good support network of women?**

**PATRICIA:**
There are women and men who pushed me. I had to find my way back and learn to be a good leader. It is vital to your sanity to have peers to lean on for support. I also find that being a mentor is critical and necessary. It’s not easy to maintain your support network when you’re working so hard all the time. But it is vital to your sanity to have peers to lean on for support. I also find that being a mentor is critical and helps you not only give back but expand your network.

**DF: What is your advice to women who may feel, for whatever reason, they’re not “good enough” to do a job.**

**PATRICIA:**
When someone asks, ‘Am I going to be successful?’ whether you have a degree in computer science, or are a mom coming into the workplace. I want to know how your skills eate to your aspirations.

First, ask yourself, ‘Am I the right fit for this job? Am I going to do it well?’ Next talk to others in the field about the skills you need to be successful and build a plan. It’s important to define what your weaknesses are, what skills you might need to develop and, ultimately, what training you may need.

I’m a ‘tough love’ kind of person and we all get to make our own choices. So, when something doesn’t go according to plan based on the choice you made, don’t focus on the negatives. You need to challenge yourself to identify what you learned from it. I’ve been fired a few times and I could have spent my time having a pity party. But instead, I turned it around, so I could really try to understand what I learned from that challenge and how it made me a better person and leader as a result.

**DF: Men see getting fired as a rite of passage, women as a badge of shame.**

**PATRICIA:**
The differences between men and women being fired, in my opinion, is women internalize it, while men just put it in a box and move on. My recommendation for anyone in any company is have an exit strategy. Some organizations are more stable than others, but all CISOs are vulnerable to one degree or another. Thankfully for me, Markel is the kind of company where long careers are not uncommon. But we must be realistic. CISOs are the first to be fired in the event of a breach and you need to be prepared for it. Especially if you are the sole breadwinner for your family. This is when the investment you’ve made in networking and building a support structure is going to get you back to True North. Security people have so much to give and so much to offer. You will not be unemployed for long unless you want to be.

**DF: You held many jobs and have had an exceptional career, let’s talk about some lessons-learned. You’ve been at Markel for more than three years now. Biggest take-away?**

**PATRICIA:**
While I’m not an insurance expert, I do need to understand what our business does so I can provide enough security. I must have an understanding of how we collaborate cross-functionally, to deploy the capabilities to protect the company.

**DF: You left the government in 2008 and joined Unisys, the global tech company. What were some of the lessons learned?**

**PATRICIA:**
It’s not easy to leave the public sector and go into the private sector. In the public sector, your value is based on the government system, so you don’t really know what you are worth in the marketplace. Unisys allowed me to work with their corporate offices and understand how the corporation worked. I think this was a huge benefit.

**DF: You left the government in 2008 and joined Unisys, the global tech company. What were some of the lessons learned?**

**PATRICIA:**
I must have an understanding of how we collaborate cross-functionally, to deploy the capabilities to protect the company.
A few years later, the CEO of Symantec reached out to you and offered you the CISO role, a huge opportunity to work at the world’s largest cyber-security company.

**PATRICIA:**
Symantec was a great opportunity to experience a fast paced, hi-tech company doing development work in other countries. This is when I learned that there are cultural implications to deploying technology in a global corporation, and you must think about those impacts. Honestly, this job helped me to stop thinking like an American and to start thinking globally.

Your next CISO job was at Freddie Mac, a private company, which at the time was under government conservatorship.

**PATRICIA:**
Freddie Mac was one of the companies where I learned many valuable lessons about leadership and management. It taught me how critical it is to be organized, build a program based on an industry framework, and create repeatable, defendable processes.

Both Symantec and Freddie Mac, ultimately were not a good fit. After leaving each organization, you took time off and traveled: Australia following Symantec and New Zealand following Freddie Mac. Each break allowed you to come back stronger.

**PATRICIA:**
Yes, I needed to think about what I wanted to do with my career. Being a CISO is a tough job and I didn’t know if I wanted to keep putting myself in vulnerable, risky positions. Over the years, I had become an adrenaline junkie. I liked working 24x7. I liked the complexities of the problems that I had to work through, but how healthy was that?

I had been in the security field continuously for 20 years and I think I was burned out. I needed to hit the reset button. At this point I couldn’t see the forest through the trees. Walking through the Australian bush gave me time to think through moments in my life. You recognize the value you bring, the things you leave, the people you worked with, the people you mentored, the lives you’ve touched, the words someone puts on paper about you, the impact on your profession, and how the work you did furthered that movement.

I had negotiated a good exit strategy, so when I came back, I was able to take time and think about what I wanted to do next. When you are leaving a company, you must negotiate a good severance deal.

I’m now in a great job at Markel. I’ve built a high-functioning team and I have time to get into strategy, financial planning and get involved in philanthropy. Recognizing my tendency to be an adrenaline junkie has helped me find a better balance in my work and personal life.

In sum, what is your best advice both in a career and in life?

**PATRICIA:**
For your career: when you are in a position of power, use it carefully and thoughtfully. In life, listen, learn, and ask for what you want. This also applies to your career. In my career, if I hadn’t asked for what I wanted, I would not have been as successful as I have been. Take a risk. Sometimes that risk pays off in undefined dividends. Also, as I’ve gotten older, I find myself standing a little further away from the edge of the cliff.

Take Patricia’s advice...

In life, listen, learn, and ask for what you want. This also applies to your career. In my career, if I hadn’t asked for what I wanted, I would not have been as successful as I have been.
TO SEE MORE STORIES ABOUT WOMEN IN CYBER SECURITY OR TO BE INTERVIEWED, GO TO:
www.consortium.net/story