“You never want your security office to be invisible.”

– Patricia Titus, VP and CISO, Symantec Corp.
Nothing Ordinary Here

CISO as strategic business enabler

It would be an understatement to say that Patricia Titus, Symantec’s vice president and chief information security officer, doesn’t have the typical high-tech executive resume. While she most certainly has the intellectual pedigree, she simply doesn’t have the accompanying academic accoutrements of most high-tech executives—no degree in computer science, physics, or business. What she does possess, beyond natural instincts and a keen sense of self-awareness, is a narrative replete with everything from experience working in both the public to private sectors to foreign service assignments in geographical locations with distinctly disparate cultures.

Titus’ story begins in rural Minnesota, when immediately upon graduating from high school she joined the U.S. Air Force to see the world with the goal of becoming an administrator via the Air Force’s Open Administration program. The Air Force didn’t see it quite that way, however, assigning her as a Morse code operator. After leaving the Air Force and giving birth to the first of two children, Titus continued to serve her country as a civilian in the Department of State and as a substitute teacher in the Department of Defense. Her entrée into technology occurred during the dot-com era, when she got on-the-job training as a UNIX programmer, Microsoft LAN administrator, and then as wireless network communications specialist before coming back to the public sector as a member of the Department of Treasury.

When the Transportation Security Administration (TSA) was formed as part of the Department of Transportation, which eventually became part of the Department of Homeland Security, following 9/11, Titus was called on to assume a new role—initially as a wireless communications expert but then as the organization’s first CISO. She left the TSA in 2008 for a series of positions with Unisys, including global CISO, before coming to Symantec in late 2011.

CIO Digest recently had a chance to catch up with Titus for an interview. It’s been approximately nine months since her appointment at Symantec, and she and her team have been very busy.

PATRICK: What does your team at Symantec look like?

PATTI: I have a team of 28 professionals. This is a bit variable as a result of new initiatives and mergers and acquisitions. We have a governance risk and compliance division, corporate security operations and engineering group, forensics and investigations team, and business integration office.

PATRICK: Because of the nature of its business, I suspect Symantec is faced with some unique security challenges.

PATTI: You are correct. We truly have a different security burden than other companies. As the largest security company in the world, we have a big target on our backs. Nonetheless, while my role may be more challenging, it is also more rewarding.

PATRICK: What were the initial steps that you took when you joined Symantec?
**Q&A**

**PATTI:** The first thing was to look at the organizational structure and to assess the needs of the business. Too often, new CISOs, when starting a new position, tend to fall back on what worked in previous lives. Rather, they need to understand the requirements of the business and what is going to deliver value for customers and employees.

**PATRICK:** There is a change taking place in how the role of the CISO is perceived. What is this about?

**PATTI:** As part of my initial fact-finding tour at Symantec, I heard that the office of the CISO was invisible to the company. You never want your security office to be invisible; you want it to be right in front as a cultural ambassador; employees and customers need to think about security every day. As a result, over the past half year, the team has worked very hard to become more visible and demonstrate their expertise—both internally and externally.

**PATRICK:** What would you recommend to other CISOs on what they can do to increase the strategic importance of their organizations?

**PATTI:** The first and most important thing is that you must get out from behind your desk. It is important to walk the lines and get out into the field—including global. Security also has cultural and societal aspects that must be understood. You must have a holistic view of security from a global standpoint and adapt to regional requirements.

**PATRICK:** To whom should a CISO report in an organization?

**PATTI:** This is a question I get regularly. The answer runs the gamut—everything from the CEO, to the CIO, to the CFO, to the general counsel. It really depends on the type of business. For a finan-

---

**PATRICIA TITUS AT A GLANCE**

**SYMANTEC CAREER HIGHLIGHTS:** Joined Symantec in late 2011 as vice president and chief information security officer. Oversees a team of 28 IT security professionals responsible for helping to protect Symantec’s infrastructure, information, and identities (people) and influencing product development.

**CAREER HISTORY:** Served three years in the U.S. Air Force as a Morse code operator in the early 1980s. Subsequently worked in various capacities for the public sector and then the private sector in the late 1990s before coming back into government in 2002 with the Transportation Security Administration (TSA). Left the TSA in 2008 and joined Unisys, eventually holding the position of Global CISO before leaving for Symantec.

**MOST INTERESTING DIGNITARIES HOSTED:** While working for the U.S. Department of State in the 1980s, Titus had a chance to spend some time with former Secretary of State George Schultz. “He was extremely personable and put everyone at ease as soon as you met him,” Titus recalls. When she moved to Africa, she met President Jimmy Carter, who had come to visit Zambia to monitor the voting process during the country’s first democratic elections. “I have immense respect for all of the work he’s done supporting democratic movements around the world over the past 30-plus years,” she comments.

**BIGGEST PROFESSIONAL SUCCESS:** Being named the first CISO at the TSA and building a security organization from the ground up.

**INTEREST IN SPORTS:** Grew up attending sporting events and playing sports. Titus relishes both the competition and the strategic planning and decisions that occur during the game. “I’m a huge Vikings (football) fan, dating back to the days of the Purple People Eaters in the 1970s, as well as a Twins fan (baseball),” she says. “Of course, hockey—the Wild—is part of my DNA having grown up in Minnesota.”

**MOST MEMORABLE MINNESOTA VIKINGS GAME:** “It was December 3, 1978 when the Vikings still played outdoors, Bud Grant was the head coach, and Fran Tarkenton was the quarterback. The Vikings were playing the Philadelphia Eagles. It was a particularly cold day and snow fell throughout the game. As we couldn’t afford anything better, we were in the cheapest section that had aluminum seating. The game had everything, including the home-stadium crowd booing the Vikings star running back off the field after he had a tantrum in the middle of the game. What was most important, however, is that the Vikings won—28–27—in the final seconds.

**FAVORITE MOVIE:** *Independence Day.* The aliens are defeated when the protagonist infects their mother ship with a computer virus. “What an ironic twist of good and bad,” Titus quips.
cial services institution, a reporting chain to the general counsel probably makes the most sense in that it is a heavily regulated institution. In the case of a healthcare organization, it probably makes sense for the CISO to report into the COO; operations are really the focus. I don’t think there’s a one-size-fits-all reporting structure for a CISO.

PATRICK: You mentioned that the role of the CISO is a bit different at Symantec; it’s a more strategic function than with other organizations. You are able to provide feedback to the business, assess potential acquisitions based on their risk, and assist in the organic development of new solutions. What is this like?

PATTI: We’re actually a customer of many of our enterprise-class solutions. As a result, we’re able to give our product groups feedback on enhancements or even the impact of new upgrades. We are truly able to impact the business and drive positive changes in our product portfolio. This real-life operational feedback delivers substantial value to customers and partners.

PATRICK: You left the TSA in 2008 and joined Unisys. What roles did you hold there?

PATTI: I started in the Strategic Program Office and worked on the security portfolio for about a year. In this role, I was able to look at the business and make recommendations on investments—internal and external—on what we should and shouldn’t do. I was then appointed Federal CISO with the responsibility of ensuring adherence with compliance standards, something critically important to our business as a federal systems integrator. I was in this role for about a year when I was named Global CISO. This gave me an opportunity to get a global view and affect organization-wide changes across our operations in all countries.

PATRICK: While you spent some time in the private sector in the 1990s, you’ve spent the bulk of your career in the public sector. What was the public-to-private sector transition like?

PATTI: Well, it wasn’t an easy one. Government has a plethora of compliance requirements. The government CISO is focused on containing on with those issues. The private sector CISO is a business enabler. Understanding this difference and making this shift has been critical to my success.

PATRICK: It was shortly after 9/11 when you started at the Transportation Security Administration? What was it like?

PATTI: It was such a serious time for the country. We were in a period of healing from 9/11 and were standing up a new Federal organization. I had a chance to work for a couple of startups in the late 1990s, and that experience served me well, as it was very much a start-up atmosphere. We had just over 200 people at the time when I came on board and grew within a few short months to 50,000-plus employees. Under the direction

“What’s really important is to select a set of standards.”
—Patricia Titus, VP and CISO, Symantec Corp.
Titus’ unrelenting work ethic was developed working alongside her father in their home garage changing sparkplugs, performing brake jobs, and overhauling engines on the family’s cars. Her uncanny ability to work across cultures and with groups and individuals of differing mindsets and levels of commitment were acquired as a diplomatic liaison in the Middle East and Africa. Her technical knowhow was not learned in the pristine halls of the Ivy League but as a Morse code operator in the U.S. Air Force and on-the-job training in the private sector during the dot-com boom.

Finally, make sure your IT organization is tightly integrated with your legal and HR teams. These groups are extended elements of the office of the CISO. They need to be included as part of policy development and investigations.

PATRICK: Connecting security and risk management back to the business and measuring risk to the business is something that every CISO must do. What does this entail?

PATTI: Continuous monitoring is vital. Technology in this equation must be positioned as an enabler of risk management. The business needs to understand and be educated on the ramifications of security. It needs to be more than simply creating a strategic business plan and compiling a final report at the end of the fiscal year. Risk management must connect back to staffing goals and objectives so that they can see how their work relates to the larger strategic plan. In our world here at Symantec, it’s about protecting people and information. I must show the ripple effect of changes in my organization and how they connect to employees, partners, customers and people across the globe.

PATRICK: The past few years have witnessed the introduction of various disruptive technologies that present substantial business advantages as well as challenges. What impact have these had on security and risk management?

PATTI: Following the dot-com era, we got comfortable for a little while. But then consumerization of IT hit us square in the eye. Some IT organizations are still in denial that it has permeated the walls of their security fortress. However,
“I must show the ripple effect of changes in my organization and how they connect to employees, partners, and customers.”

– Patricia Titus, VP and CISO, Symantec Corp.

it is here and inevitable. Consumerization of IT enables employees to do their jobs more effectively and gives them more options. The downside is that, when not properly and promptly addressed, it introduces inherent risks.

PATRICK: The cloud is something that is having a similar impact on security. How should CISOs address those challenges?

PATTI: There is a tremendous amount of potential risk with the cloud. It goes back to having a good relationship with the legal and procurement teams and making sure cloud contracts have the right compliance and audit components. Encryption is an issue that must be addressed—certain data types must be encrypted. Another challenge with the cloud is the federation of identities. Finally, once you have data in the cloud, monitoring, managing, and enforcing access to that data based on identities becomes very important.

A number of CISOs are still in pause mode in recommending the cloud to the CIO and business owners. My opinion, like mobility, is to lean into it and embrace it. The cloud will enable your business with security embedded.

PATRICK: You have been quite involved in promoting the role of women in the IT sector. Why this interest?

PATTI: I have been a member of the Executive Women’s Forum for a number of years. My interest is to influence other women to think about IT as a career path. When you sit around the table at an executive or management level and it is full of men, you get a completely different outcome when you introduce women into that environment. I received a lot of encouragement from various mentors to explore a career in security and risk management. I want to give back where I have benefited. This career field offers what many do not: challenges and out-of-the-box thinking.

PATRICK: Where do you see security and risk management heading over the next couple years?

PATTI: I see everything heading towards the application and data layers. No matter how much CISOs resist, they will end up managing data. We’ve worked hard to say the creator of data is the owner of the data. But the way data flows today, specifically its consumption, introduces substantial complexity and breaks down the wall. The responsibility for data governance and protection will shift to the CISO, who will ultimately be responsible for the protection of the crown jewels for most organizations. Data is the business, and data is the prime target!

PODCAST

Portions of the interview with Patricia Titus are available as an Executive Spotlight Podcast at go.symantec.com/titus-podcast.

I must show the ripple effect of changes in my organization and how they connect to employees, partners, and customers.

– Patricia Titus, VP and CISO, Symantec Corp.