CyberPro
Keeping Cyberspace Professionals Informed
Volume 7, Edition 4
February 20, 2014

SENIOR LEADER PERSPECTIVE: PATRICIA TITUS, CISO, FREDDIE MAC

NSCI recently had the opportunity to interview Patricia Titus, the Vice President and Chief Information Security Officer at Freddie Mac in McLean, VA. She is responsible for the protection and integrity of Freddie Mac's information assets while enabling world-class information access. Ms. Titus is also serves on the Board of Directors for Cyber United, the Board of Advisors for Blue Ridge Networks and the Technical Advisory Board for Co3 Systems. She has been writing articles on Information Security for specific publications and remains on the Editorial Board for InfoSecurity Magazine. Ms. Titus was the Vice President and Chief Information Security Officer at Symantec, responsible for IT information security risk management, threat response and governance functions. Ms. Titus played a strategic role in protecting Symantec's IT resources, infrastructure and information assets, as well as driving internal security initiatives. Prior to joining Symantec, Ms. Titus was Vice President and Global Chief Information Security Officer for Unisys Corporation, a global information technology company and formerly the Chief Information Security Officer (CISO) at the Transportation Security Administration within the Department of Homeland Security. In both CISO positions she focused on creating, implementing and maintaining robust IT security programs. Ms. Titus also worked overseas for several years in various positions within the U.S. Department of Defense, the U.S. State Department and various private sector firms. She has more than 20 years of security management experience.

NSCI: Let's start with Freddie Mac's cybersecurity posture. What area(s) are you looking to improve upon in 2014? If you had "one more dollar" in your cybersecurity budget, what would you spend it on?

Titus: We already have a good budget for security, however; I'd apply the 'one more dollar' developing a cybersecurity awareness training game. I've thought about this a lot actually as a way to enhance our existing security awareness training and to make it more engaging to our current workforce. The employee is the CISO's real front line of defense**.**

NSCI: Can you tell us about any cybersecurity awareness, education and/or training initiatives for Freddie Mac cybersecurity staff and employees? How does Freddie Mac keep its staff and employees up to speed in this ever-evolving area?

Titus: We are keenly focused on raising the security awareness bar at Freddie Mac this year. It's so important to give all our employees knowledge that will help them identify possible malware and threats with the hope that it will spill over into their personal computing time at home as well. My security team members are the Cyber Security Cultural Ambassadors at Freddie Mac who have the responsibility to help our employees understand their roles as the company's strongest front line of defense.

NSCI: What do you see as the biggest cybersecurity threats and opportunities over the next few years?

Titus: I strongly believe there has been a spike in innovation in combating the insider threat. There are more and more capabilities entering the marketplace, which mean we're going to find better ways to secure our networks from the inside out!

NSCI: The cloud continues to be a hot area regarding cybersecurity. What cloud security concerns and/or advice do you have?

Titus: There's been a lot of hype around cloud computing, both good and bad. I think the cloud providers are just as concerned about security as the companies that are investing in these capabilities. The most important thing to do when it comes to cloud computing is to write a good contract with clear requirements. And don't forget your exit plan. So many companies do so well until they realize they want to leave and they didn't have an exit strategy.

NSCI: Do you have any tips for an organization to prepare for / defend against the insider threat?

Titus: Remember not to give up on some of the basic principles of protecting against the insider. First of all, do you have a corporate policy on classifying and handling all types of data? And do you know where your sensitive data is, and how it's being accessed and used? A strong identity and access management (IAM) program is critical. I call IAM one of my *anchor programs*. Data loss prevention technology is a great addition to make an IAM program stronger. Last tip: great new companies are hitting the marketplace all the time, so pay attention to the security grapevine about the latest hot technology!

NSCI: You've been a CISO for several years and with several organizations. How have you seen the CISO's role and resources evolve during that time?

Titus: Remember that the title CISO is a relatively new C-level position, only a little over a decade old, but it has matured significantly. I've seen the CISO go from the back room to the board room in the past 5 years. The CISO more often has a seat at the table when a company is making business decisions largely because everything centers around data. Part of the evolution is that CISO's have had to learn to become 'translators'. Every day we have to translate the security threats and vulnerabilities into common language and equate it to business impacts. Thankfully, we are no longer being referred to as the 'office of No' or the 'Sales prevention office'. We are becoming business enablers. It's an exciting time to be a CISO; scary but exciting.

NSCI: You've also worked in both the public sector and private sector. How do cybersecurity challenges compare (differences / similarities) in these sectors?

Titus: The similarities are striking actually with the major difference being the compliance standards you follow. Everyone suffers from too much to do and not enough time or resources to do it all. So it becomes a balancing act and you eventually come to the realization that you cannot 'boil the ocean'.

One thing I can say is that the government, with all their challenges, has seen the value in security and I believe has taken the lead in this space.

NSCI: You are on the Advisory Council for the Executive Women's forum and on the Women's Advisory Board for the Girls Scouts Council of the Nation's Capital where you mentor young women in the IT field. How do you think we are doing with recruiting and retaining women in the cybersecurity area? Any ideas on how we improve?

Titus: This area is one my passions. . We just don't have enough women joining the IT profession and the tables are still so unbalanced. We also can't seem to keep women interested in IT if they happen to stumble into it. I think there's still the 'Dilbert' stigma that prevails today and women don't think about IT being a career path. Those of us that are in security and IT need to continually be recruiters.

I belong to the Executive Women's Forum and one of our quotes is "Lift as you rise". This is a model around my life which means it is important to lift up other women as you rise on your career journey. I want to be clear that companies do strive to hire women, it's just there aren't many in the field to hire.

NSCI: Is there anything else you'd like to add?

Titus: I want to thank you for giving me an opportunity to speak with you and for spreading the security word. It's a digital world and we've got to continue to grow and change with the technology. This means we need to continually grow our security defenses and offenses and get ahead of the threat actors.

NSCI: Thank you very much for taking the time to visit with us.