NSCI
National Security Cyberspace Institute

CyberPro

July 19, 2012

Keeping Cyberspace Professionals Informed

SENIOR LEADER PERSPECTIVE: THERESA M. PAYTON, FORTALICE

NSCI recently had the opportunity to interview Theresa M. Payton, CEO and President of Fortalice LLC. Ms. Theresa Payton is a well-known and highly respected national authority on cybersecurity, e-crime and fraud mitigation, and technology implementation. Ms. Payton has over twenty years of advanced business and security technology expertise and leadership at the highest levels of both government and in the financial services industry. She is currently the CEO and Chief Advisor of Fortalice®, LLC a security, risk and fraud consulting company serving businesses, government, and consumers. She is also co-author of the new book, “Protecting Your Internet Identity: Are You Naked Online?”

From May 2006 until September 2008, Ms. Payton served as Chief Information Officer at the White House. In this role, she provided oversight of the information technology enterprise for the President and 3,000 staff members. She oversaw dramatic upgrades to the IT security posture for the Executive Office of the President and worked closely with security assets of the U.S. Government in the civilian, military and intelligence community. Ms. Payton was the first woman to hold this position.

Prior to government service, Ms. Payton had a long career in the financial services industry, leading teams focused on improving banking technology and security. Ms. Payton has held senior leadership positions at Barnett Bank/Bank of America, Bank of America, First Union/Wells Fargo. She led strategic planning teams, managed mergers and acquisitions, ran technology operations, internet and call centers, and oversaw fraud and risk management technology operations.

Since leaving government service, Ms. Payton founded Fortalice®, LLC and has served as a key advisor to government and corporate leaders in their efforts to improve the policies, procedures, workforce, and utilization of technology to confront cyber threats. She is a member of the FBI’s North Carolina Infragard.

NSCI: Fortalice LLC is fairly new on the cyber security scene. Can you tell us a little bit about the company and what you see as its niche in this area?

Payton: I want to thank NSCI for all the great work you do to help improve awareness and arm organizations with the strategies they need to be as safe as possible online. Fortalice was founded at the end of 2008 and we are young compared to many of the wonderful companies serving industry today. We determined that there was a niche in between consulting firms and product firms where we could help organizations think differently about security. If they think of it as an expense versus a business enabler, security will “lose” to other demands. We often start conversations with execs with leading questions such as...

What if a virus started emailing your corporate secrets to the competition? Or, what if something or someone knocked out your web server for the day?
How would you deal with the negative press from a major security breach? Or, how would you deal with information leaked knowingly or unwittingly by one of your employees through social media?

Since security is a team sport now and cannot be handed to the "IT Guy" to handle, we know we need to engage the organization's leadership team early on. We typically start engagements with something very simple and non-technical to engage all roles in the organization - orchestrating the following scenario: "Have you ever practiced with your staff what you should do in the event of a major cyber incident (bank account hacked, FBI shows up and says your servers are talking to cybercriminals, your client calls and says your files are infected)?" Organizations learn a lot about themselves when they go through this exercise. Some learn their lawyers do not want them talking to anyone! Some organizations learn they would not know what to do but figure it out. The point gets across though - it is a team sport; plan and prepare.

We offer assessments, but a place where the techies love to see us come on site is in the policies and procedures area. Techies HATE to document policies and procedures. We will update them, create them, and implement them for you. We have done this for so many clients that we actually have a fast-track process called "P&P In a Box".

Another area that is critical is the Employee Education & Awareness program. Read about the latest companies that have been infiltrated and many of the breaches started with an honest mistake. An employee clicked on a link or opened an attachment and let the bad guys in. However, gone are the ho-hum days of a boring CBT (computer based training). Our employee education and awareness program is interactive, memorable, and helps your greatest asset - your staff - protect your digital assets.

Believe it or not, we also offer a "safer" social media program for our clients. We are not a PR firm, but we do know how cybercriminals leverage social media every day to trick your company into giving away its best and most valuable secrets. We have helped clients repair their reputation. We have helped clients find their weakest points, where they are either giving away their corporate secrets or they are putting themselves at digital or physical risk. We have helped them migrate to safer, smarter social media campaigns.

Regarding BYOD (bring your own device) strategic deployments, we have a saying, "BYOD without CYA creates BYOB". Bring your own device to work and housing corporate data -- without covering your assets -- creates a major headache or BYOB for managing and tracking your digital assets. We help companies deploy BYOD smartly.

NSCI: Several have stated the majority of today's cyber threats are not the result of a lack of technology, but a lack of resources. What is your view on this? What is the role of technology in helping to improve cyber security?

Payton: Chris Byrne recently spoke at the Gartner Security and Risk Summit and offered up a statistic that spells out part of the problem. Chris recommended that staffing levels for IT risk and security should be between 5% and 12% of your total staff, but many organizations have less than 3%. Technology plays a huge role but it cannot make an organization safe without help from all departments - marketing, finance, legal, and others. Investment in tools, providing your employees with policies written in "non tech" speak, education and awareness, and messages from top leadership are all critical. If an organization says "technology is responsible" but then does not support them when they register concerns that employees download large amounts of data onto portable media but instead are left without tools to track the data, it's like sending your law enforcement officers out to protect everyone but telling them to leave behind handcuffs, bullet proof vests, and all the other tools and protection they need to apprehend the bad guy.

NSCI: There's been a lot of talk about government (e.g. DoD, DHS) helping industry with cyber security and defense, especially as it relates to critical infrastructure. What are your thoughts on this?

Payton: Many of the businesses I talk to would like some assistance from the government to help protect them. There is a caveat though - they want to maintain their privacy too. Organizations such as OnGuardOnline.gov and FBI's Infragard are a great way to raise awareness. It would be great if the government could offer tools too, but many businesses comment that the tools probably would not be "leading edge" or they are concerned about "privacy" where the government might use the tool to "watch them". Although not perfect and still lots of progress to be made, I believe the Department of Defense, FBI, NSA, and DHS have made positive progress towards helping build "collective" security across the .mil, .gov, and .com. They have several venues where they talk with industry to seek their requirements and to better understand their concerns.

NSCI: Cybercrime seems to be the largest current threat to individuals, while espionage, intellectual property theft, and data breaches seem to be major organizational concerns. How do we get ahead of these threats?

Payton: I am the eternal optimist with a twist of pragmatism. On this one, I do not see how we can get "ahead" of the threats. I believe the best approach is to implement what you can so you are not seen as the weakest target but also realize that even the biggest, baddest names in security have had breaches. Plan, prepare, and practice for that worst case scenario. Sometimes the recovery plan, or lack of one, is what has been the biggest detriment to an organization.

NSCI: Numerous organizations have paid a lot of attention to educating and training the cyber workforce. How are we doing at educating the cyber citizen who routinely uses the Internet, but doesn't necessarily have a "cyber" job?

Payton: I would give us a C- if I were to grade our efforts to train Americans not in the cyber security industry, on what they can do to protect themselves. Smokey Bear teaches us that we can prevent forest fires. We also know to look left, right and left again before crossing the street. If you catch on fire you are to stop, drop and roll. How about cyber? There are a few catchy phrases but consumers are still puzzled because there is not one clear message. The media has done a fabulous job raising awareness by covering stories and issues. Several government, non-profit, and educational organizations also provide fabulous resources. For example, if you cannot afford an employee education program, there are lots of free training materials provided by organizations such as OnGuardOnline.gov. I also love the openness of the FBI to talk about law enforcement's challenges and asking the public to be part of the solution. The progress is encouraging, but results are mixed. After an extensive media blitz and outreach to warn citizens that DNS Malware changer was lurking around, the FBI reported in May that there were still roughly 300,000 devices infected with the DNS Malware changer Trojan. You could focus on the people who heard the message and acted, but why did we still have so many that did not?

NSCI: Cyberspace situational awareness continues to be a challenge for many organizations. What are the keys to improvements in this area?

Payton: Situational awareness is a noble goal to achieve, but a tool alone cannot provide an organization with focused and actionable situational awareness. I will often ask a client during our first meeting, "What one data asset would close your business if it were compromised?". Occasionally, there is a long pause before someone speaks. Other times, several people blurt out the data asset but each role in the organization has a different opinion. Rarely does the entire leadership team name the asset in unison. Sometimes organizations say "everything". I start there because if you do not know the asset you need to protect, how can you define an appropriate protection strategy? If you say "everything", you will protect nothing very well. It is too hard, too costly, and too distracting to watch every digital asset all the time.

NSCI: How do we actually measure (i.e. quantify) cyber security risk, damage, and progress?

Payton: Several organizations track this at the macro level and they all have a different opinion on this. At the macro level it is hard because you cannot tell if a metric such as "# of incidents reported" means the threats are growing or are more organizations aware and reporting the issue? At the micro level, we work with our clients to define the measures most important to them. At the most basic level we ask:

1. What needs protecting?
2. Why?
3. If it is compromised, will it shut down your company?
4. If not, what is the collateral damage?

We then look at threats, likelihood of the threats hitting that company, and the cost/complexity to mitigate the threat. That is the best way to baseline what you need to focus on and track it.

NSCI: What technology developments do you see as having the most bang-for-the-buck when it comes to improving cyber security?

Payton: I am looking forward to a day where "collective security" data elements can feed behavioral scores and tell you, or your bank, or your health care provider, or the company you are dealing with, that the interaction does not seem to be you. In addition, I would love to see the day when collective security could holistically improve security. Today, we have glimmers of brilliance with products and services that have been developed, but they are not holistic. I am also looking forward to a more effective form of authentication online that replaces id/password. I was told by a luddite once that they were convinced techies have a diabolical plot to let bad guys in and leave the good guys out by enforcing strong passwords that most of us cannot remember, but the bad guys can still hack! Better yet, the bad guys just ask for a password reset and change your account to something they can remember.

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

Payton: Thanks for mentioning that intellectual property theft is happening. America has companies HQ here like Apple, Google, and others that are seen as huge innovators. We also have amazing small companies racing for green energy, better defense tools for the US Military, and other innovations. Every company, no matter what industry you are in or size, is a target. I call IP theft the carbon monoxide of US cyber security. It's silent and deadly and you realize it when it's too late. Often many companies have something in common when they first learn something is wrong - it is a visit from the FBI to notify them they've been observing bad guys vacuuming up data from their company. A report that everyone must read is "Foreign Spies Stealing US Economic Secrets in Cyber Space", at the following link: http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf . It is one of the most thorough, well written, unclassified reports I have seen on this topic. Victims are identified and the target countries and sponsors of the cybercrimes are also noted.

Organizations like NSCI and others are so critical to fighting cybercrime. Keep up the great work!

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