National Security Cyberspace Institute NSCI

CyberPro

May 19, 2011

Keeping Cyberspace Professionals Informed

Senior Leader Perspective: Mike Saylor, Vice President, FBI Infraguard, North Texas Chapter

NSCI's Charles Winstead recently had the opportunity to interview Mike Saylor. Mike currently serves as Vice President, FBI Infragard, North Texas Chapter, and is also a member of the North Texas Chapter Board of Directors and the Cyber Crime Committee of the North Texas Crime Commission. Previous positions include National Director of IT Security and Risk Management for a national consulting firm, Global IT Audit Manager at Citigroup, and Head of Information Systems Security and Audit Compliance at a $5B global telecom.

NSCI: Can you tell us about Infragard and why people should consider joining?

SAYLOR: Infragard was initially established in 1996 to gain support from the IT industry and academia for the FBI's cyber investigation efforts. Today, the FBI sponsored program has expanded to include physical security as well as the cyber security of US critical infrastructure (CI), and the 56 individual Infragard chapters are geographically linked to FBI field office territories. Understanding that the majority of US CI is owned and operated by the private sector, through the Infragard program and networking events the FBI has developed a trusted relationship with CI organizations to facilitate more effective support and communications related to the protection of the national assets. Member benefits include: access to sensitive (unclassified) information, becoming part of a diverse network or professionals, exposure to unique and valuable training opportunities, and community involvement.

Infragard is an excellent opportunity to network with industry peers and law enforcement in an objective and neutral environment; and establish relationships that facilitate a more direct response when issues arise, such as an internal data breach, or the need to disseminate information to protect US critical infrastructure.

NSCI: What are some of the cybersecurity accomplishments of the North Texas Infragard Chapter?

SAYLOR: One of the metrics by which Infragard is measured relates to incidents or events that evolve into a federal investigation, and another objective is to promote increased community awareness and networking. In both cases, Infragard has been successful. Infragard currently has over 40,000 members and has referred hundreds of cases to the

FBI, most of which were pursued. In addition, the North Texas Chapter which has typically only held quarterly member meetings, has expanded its event schedule to include the first annual Cyber Defense Summit, partnerships with the EC-Council and their TakeDownCon event, itSMF, DFWFirst, the US Cyber Defense Center, CUISPA, ISSA, and several university cyber research and education programs in north Texas. Infragard also recently received an invitation to join the North Texas Crime Commission as part of their Cyber Crime Committee, and several other chapters are involved with similar programs.

NSCI: You've spoken on a number of topics. What do you think are the top challenges for the cyber citizen who routinely uses the Internet, but does not have a cybersecurity job per se?

SAYLOR: Complacency and awareness. Complacency with what was acceptable and safe yesterday and the lack of awareness of the evolution, maturity, and complexity of cyber crime. I speak to a lot of schools and community organizations, groups typically under educated about cyber topics, about Internet safety, identity theft, online predators, cyber bullying, etc. At the end of just about every discussion there are a number of people who ask how I sleep at night, or state how scary the world has become. My response is education and awareness, which are huge challenges for someone that does not have a cyber-related interest to maintain current knowledge of trends, issues, threats, and countermeasures. Almost everyone I meet is interested in cyber security and wants to learn more, be more diligent, and protect their kids… but rarely do any of them have the time or resources necessary to keep pace with the evolution of cyber crime.

NSCI: The insider threat continues to be an area where many organizations seem to fall short. What advice do you have for them in addressing this challenge?

SAYLOR: The industry must do a better job of educating cyber responsible resources and executives through trade magazines, conferences, etc. My experience across the US is that there is a consistent misconception that the insider threat simply is not worth addressing; with exception to those organizations that have experienced it. I have been on and around the different sides of the fence with this topic as a CISO, Internal Auditor, IT Director, and Consultant; the point can be argued but it will not go away, and with that neither does the risk, liability, and impact to the organization. In order for the insider threat to be taken seriously within an organization, 1) Business Management must understand the basic principles of the threat (most executives get this piece), 2) be able to conceptualize the manner in which the threat would be carried out (e.g. data on external HDD, emails to yahoo account, allowed to take laptop out of the country, daily trip to self storage with company boxes), and 3) most importantly they must agree on the value of potential damage, risk to the company, and the potential impact to the business. This last piece is the most difficult for IT personnel to put together without the help of the business. I highly recommend a staged approach to these three pieces of the argument. Depending on the organization, you may have to gently begin socializing the topic and then schedule more detail conversations to cover the first two pieces. During this activity it definitely would not hurt to involve internal audit. Internal Audit can be a great ally, but do not play that card to soon. Try and get as far through the executive discussion and risk and impact analysis as possible without having Audit in the room. If politics, ignorance, or anything else that typically trumps good security practices begins to evolve, then have a one-off discussion with your new best friends in Audit and strategize about how to keep the momentum going.

NSCI: Where do you see the line between network exploitation and network attack?

SAYLOR: That can definitely be perceived in several shades of grey and from different perspectives. From a technical perspective: Network attacks could include exploitation depending on the intent. Was I proving a point or making a statement; the network is vulnerable, our security controls were improperly deployed, or that impenetrable security company isn't? Exploitation typically implies that you already have access to the network either as a result of a successful attack or because it is was provided to you Mr. Insider. From a business perspective: Network attacks are noise and are best left to IT to address; just let me know if anything serious happens, like losing email. Though, there are a few occasions were large and/or consistent attacks make headlines and could affect reputation and confidence, which may prompt management involvement until the dust settles. Network exploitation is a different animal when communicating to executives. Much like the Texas A&M bonfire of yesteryear, this discussion can go from 0 to Hot in no time with potential collateral damage. Cyber security is never more important to an executive than when it fails to protect the company.

NSCI: What are the most challenging issues with information sharing between government and industry when it comes to cyber-related threats, vulnerabilities, and attacks?

SAYLOR: I believe that most IT and Cyber professionals want to communicate with the appropriate agencies, organizations, and groups when threats, vulnerabilities, and attacks are identified. I also believe they feel conflicted when they are unable to communicate these issues, which may impact company loyalty, integrity, compliance with policy, and tenure with the company. It is typically business management (e.g. legal, audit, executives) that prohibits the external communication of these topics to law enforcement specifically, and often times to industry sources as well. The challenge is unfortunately one that may never be directly satisfied, and that is addressing the misconception that involving law enforcement with respect to a specific incident may evolve into an entire internal investigation of the company's history of business. There has, however, been some progress made in addressing this issue. The establishment of intermediary trusted organizations, like the FBI Infragard, creates a networking environment of peers, industry leaders, and law enforcement whereby the casual socialization of issues can occur without formal engagement.

NSCI: Cyber crime continues to be a major threat to Internet users. What are the keys to making significant progress in this area?

SAYLOR: My brother in-law was the Army SF ISO in Afghanistan; as a result, he is now a professional poker player. My point is that if you can develop a security and risk conscious mindset and employ that in your daily life, not only will you begin to see things differently, but you will inherently reduce your exposure to threats. Having said that, I also believe there is currently a generation gap with Cyber Security education. Most of the population above 50 has little to no understanding; 30 to 50 saw cyber security evolve; 18 to 30 are on the cutting edge; and those under 18 are more focused on convenience and instant gratification to care (a bit biased here with a 15 yr old daughter). A few suggestions – 1) have at least two email accounts, one for all your personal business (online banking, PayPal, eBay, cell phone, etc) and second trash account to use for everything else. This will likely keep spam and phishing attacks focused on your trash account. 2) Limit the use of personal information on the Internet to extent possible. This includes applications, social media sites, networking sites, chat sessions, photos, reviews, etc. The more information someone can compile about you, your family, and your activities the more effective their attack will be. 3) Practice safe computing and clean desk / counter policies at home; open windows, doors, recycle bins, and vehicles are easy prey. 4) Do not allow your computer to save password, Internet history, or cookies. 5) Ensure your home network is configured to provide the maximum security your equipment can support; or purchase better equipment. 6) Install and use anti-virus. 7) Do not visit websites of questionable content. 8) Do not download files from questionable websites, including movies, MP3 audio, pdf documents, photos, etc; these can easily be modified malware. 9) If you see something on the Internet that looks too good to be true… it is and you will learn the hard way if you fall for it (visit www.lookstoogoodtobetrue.com). 10) Install some type of Internet Safety application on computers your children use (e.g. K-9 by BlueCoat is free). Configure Internet Safety applications to restrict Internet use to appropriate times of the day (not 1am), and block inappropriate content, language, search results, etc. We may be diligent adults, but one 15 yr old daughter modifying her MySpace page can infect a home computer with tons of malware. 11) Understand that it is a fact that there are no executors of estates in other countries that need your help funneling inheritance monies into the US; and furthermore, if a foreigner truly won millions of dollars in a US lottery he would likely invest in the relatively inexpensive trip back to America to claim his winnings. 12) Lastly, common sense is worth every penny, do not be naïve just because you are online. (Visit www.stopthinkconnect.com & www.staysafeonline.org for more tips)

NSCI: What should state and local authorities be doing to improve cybersecurity at their level?

SAYLOR: There are a few current initiatives sponsored by state and local organizations to address their cyber security objectives. One of the keys to being successful as a nation is communication. If organizations, agencies, industry, and communities would share their successes and failures then we could get to a better cyber security posture more efficiently and effectively. I believe there are a few initiatives that include information sharing, networking, and pseudo partnerships aimed at building synergies and addressing common goals and I have seen the occurrences of these arrangements grow over the past few years. State and Local agencies should look to industry experts for help, share successes and failures, partner to the extent possible, and become involved (integrated) with the Cyber community. A few initiatives are working to address some of these issues. The North Texas Crime Commission – Cyber Crime Committee discusses and supports ways to address cyber crimes at all levels in the North Texas region. This committee is made of local, state, and federal law enforcement, Cyber experts, Corporate representatives, University Cyber Program Directors and Researchers, and members of the intelligence community. The FBI Infragard is not to dissimilar with membership representation consisting of federal, state, and local law enforcement, corporate professionals, federal, state, and local emergency response personnel, Program Directors from University Cyber programs, and many others.

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

SAYLOR: Cyber security professional thrive on the challenge of understanding and addressing the current threat, educating others in some cases, and in other cases being a part of finding the next zero day. Everyone else will likely become a Cyber Security professional as a result of being exploited.

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