CyberPro

August 11, 2011

Keeping Cyberspace Professionals Informed

Senior Leader Perspective: Sanjay Bavisi, EC-Council

NSCI's Charles Winstead recently had the opportunity to interview Sanjay Bavisi. Sanjay Bavisi is the Co-Founder and President of EC-Council which was formed post the 9/11 incident where issues of cyber terrorism were raised in the forefront of security of nations at large. Jay, as he is popularly known, regularly shares the platform with Legislators and Policy makers, to Senior Officials of Government Agencies and Educators at various international conferences and seminars. Sanjay is a distinguished and popular speaker on Information Security, and presents regularly at Interop Las Vegas, CSI, Techno Security, and Techno Forensics. Jay was also the Chairman of the Keynote Hackers Panel at Infosecurity Europe 2008, the Closing Keynote Speaker for ITWeb Security Summit, South Africa, and also the combined Keynote Speaker for Techno Security/ Hacker Halted USA 2008. He has appeared regularly on several local and international television shows and print media. Having always championed Ethical Hacking and Countermeasures, Jay is also a prolific writer, having contributed regular articles and is currently a contributing author for an information security handbook due this year by El Selvier. He has the distinction of having worked as lead negotiator in securing several e-business projects for an established IT solutions company specializing in Customer Relationship Management solutions. He was the conference Chairman for the Inaugural International "Hacker Halted" Conference which was officiated by the then Honorable Deputy Prime Minister and Minister of Defense of Malaysia. Sanjay Bavisi is a law graduate from the University of Wales, College of Cardiff, having an LLB (Hons), Barrister – at – Law from Middle Temple, London.

NSCI: First, can you tell us a little bit about the EC-Council and the priorities you have for 2011?

BAVISI: The International Council of E-Commerce Consultants (EC-Council) is a member-based organization that certifies individuals in cybersecurity and e-commerce, and we do so through over 20 certification programs offered by over 450 training centers in over 87 countries. We've trained over 100,000 professionals and certified over 40,000 members. We also organize international conferences, such as our flagship Hacker Halted series, and our brand new technical IT security conference series, TakeDownCon, which debuted this May in Dallas.

As for our priorities this year, we have many new things taking place. We have two of our conferences coming up: Hacker Halted Miami and TakeDownCon Las Vegas. These events will feature the best and brightest cybersecurity professionals, and really capture the essence of what EC-Council is all about. In addition, our new Center for Advanced Security Training (CAST) debuted this year, so we'll be working closely with our CAST trainers to further develop this program and expand its offerings. Certified Ethical Hacker (CEH) is now in its seventh version, and we'll continue its international rollout this year.

And that's not all. We're also planning initiatives to help create a better prepared, and more informed, CISO community, as there's never been a greater need for strong guidance in light of all of the recent attacks. You might remember that Sony didn't even have a CISO prior to their massive breach, which is evidence of the need for this initiative. As part of this initiative, we are creating a CISO certification. But we don't just want to focus on the corporate world; we want to help the academic community too, including the K-12 and university segments, in line with the Obama administration's cybersecurity plan. The goal is to help shape youths' understanding of digital safety, ethics, and security, so that they'll be prepared to enter the workforce.

Lastly, we're excited about a new "Global Cyberlympics" event this year that looks to bring together, and reward, the best of the best in cybersecurity.

NSCI: We hear a lot about the need for a larger, better qualified cybersecurity workforce. How many people per year take EC-Council training or receive an EC-Council certification?

BAVISI: There most definitely is a need for a larger, better qualified cybersecurity workforce, and we are seeing growth on our end. We certify over 10,000 people each year, and that number is growing steadily.

NSCI: Are the EC-Council Certifications recognized by the Department of Defense and/or other organizations with similar cybersecurity workforce standards? Does EC-Council work with the organizations when they are establishing their standards?

BAVISI: Our Certified Ethical Hacker (CEH) program has been accepted by the Department of Defense's Directive 8570 as a baseline certification for government personnel holding information assurance positions; more specifically, it covers the Computer Network Defense positions of Analyst, Infrastructure Support, Incident Responder, and Auditor.

In addition to the Department of Defense, our certifications are also recognized by the National Security Agency. CEH is recognized by NSA/CNSS 4013 Advanced (Systems Administrator). Our Computer Hacking Forensic Investigator (CHFI) is recognized by NSA/CNSS 4012 Senior Systems Managers. In fact we have other certifications that meet the CNSS 4011 – 4016 standards.

We have made an application to ANSI, the American National Standards Institute, in establishing our standards by ensuring that our certifications are ANSI 17024 compliant, since they are essentially the voice of voluntary consensus standards in the United States.

NSCI: How have the EC-Council Certifications and Training evolved to keep up with changing vulnerabilities, threats, and risks?

BAVISI: Our Certified Ethical Hacker program is now in its seventh version, which includes new additions that reflect the evolution of, and advances in, cybersecurity threats. Even our trainers at our new

Center for Advanced Security Training (CAST) will adapt their material along with changing threats. All of our certification and training programs go through this process, with each new version serving as a snapshot of what's relevant at that time. As new tools and techniques surface, we incorporate this into our training, so that students are as current as the hackers they're preparing to defend against.

NSCI: The EC-Council also serves as host to the annual Hacker Halted Conference. When is the next one and what goals do you have for it?

BAVISI: The next Hacker Halted will be from Oct 21-27, again in Miami, FL. The objective of the Hacker Halted conference series is to raise awareness towards increased education and ethics in information security. This will be the 3rd time we are hosting the event in Miami, and with keynote speakers such as Bruce Schneier, Jeremiah Grossman, Philippe Courtot and George Kurtz among others, it will be the perfect learning and networking platform for information security professionals from all around the world.

NSCI: The Department of Defense is rapidly adding or modifying cyber-related training for many of their employees. How would you like to see the DoD, and government in general, better leverage commercially available cyber training and certifications?

BAVISI: The Department of Defense has taken a great step by accepting vendor neutral certifications, like CEH, which are developed by security professionals, and involve real-world, hands-on tools and techniques. As aforementioned, the DoD accepted our Certified Ethical Hacker program for information assurance personnel. One way to better leverage this training is by getting non-security staff involved in the training process, since a lot of attacks can begin by, let's say, an administrative assistant opening up a nefarious attachment; there are certifications like our Security 5, for example, that educate non-security personnel about security. To sum it up, to better leverage this training, they should get more employees involved in the security process.

NSCI: There's been a lot of talk about some sort of "driver's license" for the Internet. What are your thoughts?

BAVISI: This would be a disaster. What would the requirements be? It would seem that the overall goal of the license is to establish some sort of security education among the Internet's user base. However, how effective would a one-size-fits-all license be, if your grandmother, who might check her e-mail from time to time, can pass the test to get it? On the other hand, what if we find that the most effective driver's license is too hard for the average Internet user to obtain? No more e-mails, tweets, or Facebook status updates for them?

Obviously, it's unreasonable to expect the general Internet user to understand computer security, and by requiring a license to use the Internet, you're going to alienate a gigantic portion of the Internet's users, which, in theory, would kill the Internet economy. Security needs to be built-in, turned on by default, and transparent to the user; it's not up to the user, and if we leave it up to them, there's nothing a license can do to keep it from turning into a catastrophe.

NSCI: I think there were over 50 cyber-related bills introduced by Congress in 2010. What do you think the priorities should be regarding cyber legislation?

BAVISI: The priority should be accountability for poor security policies. There's no liability these days when security falls apart, and I think it's long overdue that we enforce hefty penalties on organizations if their security infrastructure falls apart because of negligence. Compliance regulations are a good start, but we need to give more attention to how this scales from everyone from the federal government to the small business. In addition to this, there absolutely must be more awareness for the importance of increased education and training – especially in the face of opponents like Anonymous and LulzSec. Advanced training should be as mandatory as maintaining compliance; after all, in order stay compliant, you need to stay current.

NSCI: What incentives, or penalties, do you think are needed to increase private sector cybersecurity investment?

BAVISI: Security doesn't bring in revenue, but it costs, which is why many organizations are reluctant to invest – especially if they've never been attacked before. Compliance regulations have forced these organizations to care about security, by imposing penalties if they fail to meet certain requirements, and I think we need to be stricter about this. The Department of Commerce recently published a green paper, stating that we should also reward companies who put forth effort to maintain compliance; if they still fall victim to an attack, we should consider lessening the penalties. This green paper, titled, *Cybersecurity, Innovation and the Internet Economy*, is a step in the right direction, since it aims to guide the federal government in efforts to help the private sector formalize best practice standards, gain more awareness for increased education and funding, and provide incentives for maintaining compliance. Attacks will happen, compliant or not, and we need to be swift and consistent with penalizing organizations who don't care – while providing some level of consideration to those companies that try to manage better IT security practices but still fall victim to attacks.

NSCI: In addition to the cyber workforce, we need to educate the cyber citizen who uses the Internet daily but may not necessarily have a cybersecurity job. Does EC-Council have any initiatives focused along these lines?

BAVISI: We do, actually. Our "Security 5" certification is great for people who have as little knowledge of computers as being able to check e-mail and surf the Web. This course teaches them the foundations of security, how to recognize threats, how to use the Internet safely, how to administer Windows securely, and what to do in the event that they realize they've been attacked. It's comprehensive enough to cover all the bases of how to secure the general use of computers and the Internet, and intuitive enough for them to grasp easily, as a general user.

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

BAVISI: Yes. In closing, I'd like to again stress the importance of cybersecurity education and training. Before we can do anything successfully, we have to understand how it works, and far too often, we're seeing attacks that thrive on cluelessness. We're going to have to better train our IT security staff, and this training, as I emphasized before, needs to carry as much weight as compliance does today – in fact, it should be mandatory.

This plays a big role in our initiative to assist with educating children, too, and enhance cybersecurity education from the elementary school level, all the way through the university level. Security is very much a way of thinking, and it's crucial to get minds thinking early. Being more proactive with training can prevent a lot of disasters in the future, by keeping personnel as current as hackers are. A better prepared staff equals better compliance, and better compliance leads to a better defense. Good security decisions begin with a well-educated, trained, and prepared security team.

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