CyberPro

February 23, 2012

Keeping Cyberspace Professionals Informed

SENIOR LEADER PERSPECTIVE: EDDIE SCHWARTZ, RSA

NSCI recently had the opportunity to interview Eddie Schwartz, Chief Security Officer at RSA. Mr. Schwartz has 25 years experience in the information security field. Previously, he was CSO of NetWitness (acquired by EMC), CTO of ManTech, EVP and General Manager of Global Integrity (acquired by INS), SVP of Operations of Guardent (acquired by VeriSign), CISO of Nationwide Insurance, a Senior Computer Scientist at CSC, and a Foreign Service Officer with the U.S. Dept. of State.

Mr. Schwartz has advised a number of early stage security companies, and served on the Executive Committee for the Banking Information Technology Secretariat (BITS).

Mr. Schwartz has a B.I.S. in Information Security Management and an M.S. in Information Technology Management from the George Mason University School of Management.

NSCI: You've been in the cyber security business for quite a while. What are a few of the most significant changes you've seen in recent years?

Schwartz: The greatest changes are in two areas. First, leading organizations have shifted from a security program and investment focus that is driven by compliance to one that is centered on protecting the most important information assets against a range of very capable cyber adversaries. Secondly, leading security teams have moved from a position of simply trying to confirm problems that are already known to a proactive stance in which security intelligence drives their priorities, behaviors and program outcomes.

NSCI: Where can the private sector most help the nation as a whole in improving cyber security? What are the challenges with actually doing it?

Schwartz: There are a few elements to improving the situation. First, organizations need to rethink their security programs along the lines of the changes I mentioned. Secondly, greater collaboration is required – among peers, across industry sectors, and across public and private boundaries. Sharing of real-time indicators of compromise in a collaborative framework is yielding spectacular results in some sectors. Finally, public policy must evolve to support collaboration without liability constraints, but also force the hands of some organizations that just will not come to table.

NSCI: What are a few of the improvements we need in forensics capabilities to ensure more timely assessment and/or attribution are possible?

Schwartz: Historically, security has been a very reactive discipline. Each new threat has triggered a new technology. Thus, the data center of many organizations is a collection of various security appliances and technologies, none of which share the same data schema, performance characteristics, or analytic capabilities. We have to evolve to an approach that is "big data" oriented, similar to other information management disciplines. This approach requires a few elements: a high performance, distributed data storage strategy since we'll be pulling in full packet data, log data, and other information at the app layer from all kinds of systems. We'll also need to normalize all the data elements in a way that is meaningful and accessible to security, audit, and other authorized users. Finally, we need better visualization and analytics. I believe we've see some great improvements in tools for network investigations and forensics, but we need more automation and these tools needs access to the normalized big data I described in order to achieve true situational awareness.

NSCI: What are some of the keys to successful cybersecurity risk analysis and response? What are the critical challenges?

Schwartz: The keys and challenges to doing risk analysis and response with regards to today's threat landscape are two sides of the same coin. This is because the imperative is one that upsets the apple cart and change is difficult. We need to move away from a traditional security mindset that has become heavily dependent on technology and automation. To put it bluntly, the time of "Security for Dummies" is over and it's time to get our hands dirty and invest in our people as much as we invest in our technology. At the core of this is no longer waiting for our technology to tell us we have to act. We need to proactively analyze our complete environment with regards to the threats against it and be able to recognize deviations from good, not the advent of bad. Much like a military intelligence approach, we need to have tools that allow us to dig deeper and manipulate all data. From a personnel standpoint this requires an expansion of some current skillsets and the addition of new skillsets, such as network investigation and data modeling/analysis, which are not currently widely understood by security folks. We need hunters, not responders.

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

Schwartz: The interesting thing about measuring security success is that many view measurement as binary. If you're not hacked, your security must be adequate, if you are, then you've failed. What the world has come to see abundantly over the past few years is that the picture is far more complex. Some of the most damaging attacks have been detected quickly, while others can lie for literally years undetected, giving a false sense of security. What this underscores, is that risk is universal and that constant analysis and assessment is required.

From a measurement standpoint, the historical approach is Risk = threats x assets x vulnerabilities. This is flawed in that not all assets are equal, not all adversaries employ the same tools, and trying to defend every point of vulnerability with equal priority is a losing proposition.

To understand risk, and do so in a "best practices" manner we need to understand two elements. First, what assets do we have and which represent the potential for greatest damage to the organization. Understanding that even low level assets can be a gateway to more critical systems, we need to understand and protect the ultimate target before we try and secure all of the potential paths to it.

Second, we need to understand and be aware of the overall landscape of malicious actors and commonalities between successful attack methods. Though the specific tools may differ, understanding the approaches allow us to be more proactive in architecting a defense.

As for measurement of progress, it's like your parents told you, you need to learn from your mistakes. Failure is instructive. As attacks happen, organizations need to examine if and how they are getting better at predicting attacks and post-attack detection. If an organization can track at what point they detected an attack, they can compare that with previous attacks. If the detection window is shrinking, then you're getting better.

NSCI: Some have stated that cyber defense will never be perfect and may be reaching a point of diminishing returns, thus cyber offense should also be considered. How do you view the balance between defense and offense?

Schwartz: This is an area of discussion where the risks in many ways far outweigh the benefits – especially in light of the fact that there are laws against many of the actions that would fall under "offensive" cybersecurity.

Let me come at this from a different perspective. First and foremost, in my opinion, commercial and government entities need to focus on network defense in infosecurity programs. While not perfect, as no solutions are, I think it is proven as the most effective way to repel attacks and defend assets. And to be blunt, pursuing a level of vigilantism is taking your eye off the ball in my estimation.

However, there is something to be said for taking an offensive mindset, or more appropriately understanding the mindset of your adversary to architect a better defense. As an industry we spend a lot of time trying to close doors after an adversary has already come through them. If we assume our adversaries will use specific information, and understand how it can be used against us, we can better arrange our processes, policies and deployed technologies for an effective defense. We also need to be proactive in exploiting the information and intelligence available to us to proactively adjust security posture.

NSCI: How would you say the government is doing with regards to collaborating with industry to improve cybersecurity? Any recommendations for improvement?

Schwartz: The US government has made great strides in improving public/private partnerships, in particular looking at what the Department of Homeland Security has done with vulnerability and threat indicator data. DHS has also done great works in partnership with Defense Industrial Base companies to create collaborative security frameworks – and those frameworks are being expanded into other sectors such as financial services.

The next logical step is to take these efforts globally and drive for adoption of international standards in machine readable intelligence. The goal is to securely enable security information sharing at a machine level for rapid integration and implementation of intelligence.

NSCI: Many have talked about a potential "Cyber Pearl Harbor," specifically as it relates to a major cyber attack on our critical infrastructure. How real would you say this kind of threat is? What additional action should we be taking right now?

Schwartz: I'm not one for hyperbole or sabre rattling so trying to draw correlations at that level is not something I'm comfortable with. However, the reality is that everything is vulnerable at some level and the more important it is, the bigger the target it is. So to that end, we should never be over confident and should always expect the unexpected. We know with a high level of confidence that nation states and other adversaries have targeted infrastructure concerns. So it just stands to reason that we need to understand what needs to be protected and expect that someone will likely test that protection.

NSCI: There has been a lot of concern that the United States does not have enough skilled cyber professionals. You've held key cyber security positions at many organizations. What's your view on the problem and possible solutions to it?

Schwartz: The issue of skilled professionals is not just a US issue, it's a global problem in my view. As I noted previously, in a world of advanced adversaries and threats, we can't suffer technology dependence to fix our problems. We can't automate ourselves out of danger. If we have any hope of improving our security situation, we need to be able to take the battle to our adversaries. We need to expand existing security disciplines, and embrace related disciplines such as "big data" scientists; law enforcement/military intelligence. And these skills and connections need to begin at a university level and be grown and supported through extensive professional training.

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

Schwartz: Honestly, today, the best technology strategy is one of the oldest and most proven technologies in existence – the human mind. Historically, forward leaning security organizations have built their security strategy around three analytical pillars – security information and event management, network behavioral analysis and some mix of manual processes and custom software for parsing data. What we need to see are more analysts at the center of this. Analysts, when armed with the right arsenal of tools, can focus a combined technology set. This again, is upending a bit of how we currently view security tools. We need to stop "point product" thinking, and arrange strategic components into a larger solution with big data analytics on the back end.

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