BY RAY COULOMBE

IT Security in the Spotlight

Highlights from the recent PSA Cyber Security Congress

In January I had the privilege to attend PSA's first Cyber Security Congress. PSA is aggressively taking a lead role in initiating an industry conversation and awareness of cybersecurity issues. Why PSA? The answer lies in its commitment to its owners, members and partners to educate and position them to deliver the highest level of security to their customers. Today, that must include cybersecurity. Although it is impossible to distill two days of content into a couple of page, I thought it would be worth touching on the highlights.

That the threat is pervasive is of no doubt. David Brent of Bosch cited statistics indicating 40,000 advanced attacks in 2013 with 60,000 malware variations introduced every day (malware is the term for programs embedded into a computer or system designed to compromise or co-opt that machine immediately or later upon command). He discussed the StuxNet virus, created to cripple Iranian nuclear centrifuges through Siemens PLCs that subsequently escaped into the World Wide Web. It has now apparently made its way onto the International Space Station. He also mentioned REGIN, an advanced piece of malware, described by Symantec as "a multi-staged threat; and each stage is hidden and encrypted, with the exception of the first stage. Executing the first stage starts a domino chain of decryption and loading of each subsequent stage for a total of five stages. Each individual stage provides little information on the complete package. Only by acquiring all five stages is it possible to analyze and understand the threat." Symantec's whitepaper on the subject can be found on its website.

Among the advice offered, here are five of the key take-aways:

1 **Create a Cyber Incident Response Team (CIRT) to respond to cyber events.** CIRT is an internal multi-disciplinary team involving all potential stakeholders — including executive management, IT, security, legal H.R., finance and public relations.

2 **Understand prevailing privacy laws which address people's rights and expectations of personal privacy in the workplace.**

3 **Proactively and reactively address potential, suspected or proven insider threats with policies, audits and personnel assessments.**

4 **Conduct regular penetration and vulnerability testing.**

5 **Invest in employee education and training, particularly with respect to social engineering.**

Other Cyber Issues

Darnell Washington discussed future cyber-hardened IP cameras, foregoing the use of user names and passwords in favor of digital certificates provided by the end-device. He advocates multi-factor authentication and strong encryption of the data stream — capabilities that will be required by the Federal government.

Attorney David Wilson, CISSP, discussed the very real responsibilities organizations have in terms of policies, procedures, risk and vulnerability assessment and management, data access and incident response plans. Failure to address these issues can create not only technical vulnerability, but legal exposure, as well. Increasingly, organizations will have to show that they have taken all reasonable precautions and actions towards cyber attacks to bolster a potential legal defense.

Insider threats constitute a significant, continuing exposure for all organizations, whether disgruntled or terminated employees, contractors or someone on the take. Daniel Velez of Raytheon detailed nine steps to managing insider threats. Significant among these were establishing an insider threat program and the underlying business case including audit requirements; proper staffing, arguably more important than the technical controls; getting input and buy-in for the program from stakeholders — IT, Security, HR, unions, legal and others; thorough documentation and concept of operations; selection of supporting tools; and, having an implementation plan that includes a corresponding plan from vendors to encompass help desk and training.

Charles Tendell's session on Hardware Hacking demonstrated Shodan (www.shodanhq.com), a search engine that discovers just about any device connected to the Internet.

In the session *"Anatomy of a Cyber Breach,"* Frank Hare of Red Team offered some tremendous insights into the world of a cyber breach. Check out http://map.ipviking.com, published by security company Norse, that shows in real-time where cyber attacks are coming from around the world. He noted Verizon studies that show that 89 percent of all attacks would be ineffective if users were properly schooled on what to look for in email and messages. His recommendations for a hardened cyber defense include forensics, training and policies; collaboration; and multiple layers of protection that includes an organization's vendors.

How Integrators Can Take Advantage

For a significant number of attendees and readers of this column, the question comes down to what value and opportunities result from an IT security-based relationship with a customer. Where do customers turn for IT security solutions? Should it be IT resellers, security integrators or someone else?

Kirk Nesbit of Synnex Corp., discussed managed service opportunities in this new world of cyber threats, in terms of the components of IT Security — People, Process, Technology, Administrative Controls, Physical Controls and Technical Controls. A security integrator can potentially play — starting with vulnerability assessments and penetration testing, addressing discovered gaps, and then moving into ongoing managed services.

Integrators who want to take advantage of this opportunity need mindset, strategy, training and staff. Dean Drako of Eagle Eye suggested that initial opportunities for security integrators with their customers may have to be pursued on a limited-scope basis, earning credibility step by step. Integrators are well positioned because of the diverse systems — each with their own potential issuers — that they pull together.

I congratulate PSA for taking the step to elevate this dialog. While the Cyber Security Congress was targeted at management, PSA-TEC, held in Westminster, Colo., from May 5-8, has been expanded to create a cyber track targeted at its integrators' technical disciplines. Check it out at www.buypsa.com/Education/PSA-TEC. ■

Ray Coulombe is Founder and Managing Director of SecuritySpecifiers.com and RepsForSecurity.com. He can be reached at ray@SecuritySpecifiers.com, through LinkedIn at www.linkedin.com/in/raycoulombe or followed on Twitter @RayCoulombe.