the cyberwire

The CyberWire
621 East Pratt Street, suite 300
Baltimore MD 21202–3140
editor@thecyberwire.com
www.thecyberwire.com
@thecyberwire

RSA 2014

February 24-27, 2014 San Francisco, California

February 24

RSA opens today. The conference is just getting underway as we publish today's issue, but some themes worth your attention are already emerging and several of them are linked. Expect to hear much discussion of advanced malware detection and defense. Expect also to hear about the challenges of security labor force development. Mobile and cloud security will continue to engage conference participants, as will threat analytics and next-generation network defenses.

Amid a general sense that the advantage has shifted from defense to offense (bad actors, being unconstrained by little beyond the black market's rough and uncertain frontier justice, seem able to stay a step ahead of defensive measures), we expect to hear much about how enterprises can keep pace with or even anticipate advanced threats. Current security practices depend heavily on what Dark Reading calls "super-techies": scarce and consequently high-priced engineering talent. We also expect to hear about ways to ensure an adequate pipeline of security talent.

Automated tools, particularly those well adapted to performing complex malware reverse engineering, will be of considerable interest. Such tools, in principle, could address both the rapid evolution of threats and the relative scarcity of high-end security talent.

Many conference attendees will offer their take on threat analysis, with a number of solutions already queued up for public launch this week. Look for ways of addressing anonymized threat information sharing, arguably the long pole in this particular tent.

Special coverage of RSA Conference 2014 continues through February 28th. If you're attending RSA, be sure to stop by CyberPoint's booth (#1037 in the South Expo hall) and say hello to the CyberWire's publisher and some of our stringers.

February 25

Richard Clarke, member of the President's Review Group on Intelligence and Communications Technologies, addressed the Cloud Security Alliance Summit yesterday at RSA. He described "policy failures" and their consequences, drawing particular attention to what he characterized as disconnects between policy-makers and operators. One of the consequences he discussed was the headwind security fears have imposed on US IT exports. In some respects little more than a new form of familiar FUD, such concerns have given rise to ultimately futile and wasteful gestures toward national cyber autarchy. These have as little prospect of success as did earlier autarchic programs in other sectors. Clarke called for greater transparency in intelligence policy (internationally as well as in the US) and strongly advocated for the encryption of data "in transit, at rest, and in use." (Compare Clarke's remarks with the White House's just announced consultations on privacy and technology with MIT.)

The Innovation Sandbox results were announced yesterday and congratulations go to the overall winner, Baltimore's own RedOwl Analytics, the pride of Light Street and leader in enterprise situational awareness. The other finalists deserve honorable mentions (and your attention) as well: White Ops (bot detection), Bluebox Security (enterprise mobile security),

Cylance (advanced malware identification), Co3 Systems (incident response automation), ThreatStream Inc. (collaborative threat intelligence), Skycure (mobile security), Defense. Net (DDoS mitigation), Light Cyber (predictive breach detection), and Cyphort (detection and analysis of next-generation threats).

February 26

Surveillance policy and its discontents garner expected attention. RSA's Art Coviello describes a "historic" shift in IT capability and usage and calls for international collaboration among governments and industry to arrive at new, satisfactory norms for a new digital era. He also has some criticism for the NSA (and some RSA exculpation) as he advocates breaking the agency up. See news from the parallel TrustyCon for elaboration and counterpoint.

Encryption has emerged as the RSAC's motherhood issue in major addresses, with Bruce Schneier effectively seconding Richard Clarke's admonition to encrypt wherever possible.

Computer World glumly sees the heavy attendance at RSA as a sign the hackers (the bad ones, not the good mavericks) are winning, although it does admit it's also a sign of a healthy cyber security sector. At Security B-Sides, Trey Ford makes an "impassioned" plea for hackers (the good ones) to get involved and start influencing legislation to unshackle creative security potential.

And, of course, many new products, solutions, and services are announced.

February 27

Juniper Network's security business GM treated RSA symposiasts to a stem-winder on the various cyber threats that enterprises face. Some journalists described his talk as a "call to arms"; in any case, he certainly made an unambiguous (albeit general) case for active defense. Other industry leaders prescribed less aggressive but equally ambitious solutions to the limitations of legacy security models: continuous threat protection, automated detection and response, chip-based security, and anonymized information sharing all gain a hearing.

Many of the speakers have dealt with what TechTarget describes as "information security mistakes" in policy, technology, and technique. Bruce Schneier (again, advising encryption) offered an appraisal of state capabilities that seems (perhaps surprisingly) more balanced and less alarmist than Richard Clarke's. Code Pink and DEFCON offered their own commentary as propaganda of the deed (deeds poorly received, apparently, by many of those attending RSAC).

US FBI Director Comey decried the difficulty of information sharing, which he sees as impeded by technical and legal obstacles. He hopes someday to make attack information as readily available to concerned parties as, say, fingerprints currently are to law enforcement agencies, but acknowledges there's considerable work left to be done.

The legal obstacles—privacy protection, IP protection, and even laws against anti-competitive collusion—are not, as several speakers note, inconsiderable: here, again, advances in anonymization would appear to offer a partial way through.

Director Comey's colleagues in the US Secret Service describe themselves as interested in the prevention and deterrence of cyber crime, not merely its detection and punishment. Dell reports one trend in cyber crime: crypto-currencies are offering criminals a new and growing sphere of activity, with more than one hundred varieties of malware now looting Bitcoins and other alternative currencies in the wild.

Several companies exhibiting at RSA offer a fresh approach to cyber workforce development: a vocational exploration called LifeJourney. SafeNet, Symantec, CyberPoint, Lockheed Martin, Trustwave, Intel, CompTIA, COPT, and Hexis are among those offering some of the fifty LifeJourneys running in 2014.

February 28

RSA, which has seen record attendance this year, has also spawned a crop of collateral or competing conferences.

One of the more interesting competitors, TrustyCon—effectively a protest against alleged industry complicity in government surveillance—met yesterday, and we link to some TrustyCon stories in the RSA section below. Legal observers at TrustyCon think Lavabit was "no unicorn," and that we'll see similar legal pressure to breach privacy expectations in the future. Google engineers call for the "Certificate Transparency" their company has advocated (and worked toward) as a means of reducing risks associated with certificate-based threats. Other symposiasts warn that automated update services may represent the next surveillance attack vector.

The split between the two conferences mirrors a divide in the cyber sector itself, into what might be called its libertarian and national security wings. The split is by no means clean and unambiguous—many, arguably most, companies bear feathers from both wings. Both camps advocate encryption, and both find much to love about anonymity (and anonymization).

Richard Clarke thinks fixation on perimeter defense left NSA vulnerable to Edward Snowden's insider threat and the disclosures that opened, for good or ill, this divide. (Those disclosures have made changes in surveillance policy inevitable, as news from outside RSA 2014 suggests: see stories on GCHQ webcam snooping and NSA Director Alexander's expressed willingness — in what may have been his last testimony before Congress as Director — to change the direction of his agency.)

Other RSA 2014 presentations covered the challenges of getting C-suite support for security. CISOs are warned on the necessity of anticipating breaches to prepare for disclosure, mitigation, and remediation. The realities of cloud security are said to be less grim than widely thought, but also more poorly understood than hoped. Industry trends include the rise of "spooks-as-a-service" and the security uses of big data.

The expected exploit demonstrations and product launches continue: some of the more interesting arelinked in the daily issue.

the cyberwire

editor@thecyberwire.com
www.thecyberwire.com

@thecyberwire
+TheCyberWire

About The CyberWire

The CyberWire is supported by CyberPoint International and its community partners. We invite the support of other organizations with a shared commitment to keeping this informative service free and available to organizations and individuals across the globe.

Revised 8.4.15