USA RSA Conference 2015
San Francisco, CA
April 20-24, 2015

M. R. Pamidi, Ph. D.
Editor-in-Chief
Keith Brown
Managing Editor
IT Newswire

Executive Summary

With the recent individual and rogue states-sponsored attacks on major retailers, banks, and the public sector, cybersecurity continues to be a major privacy and security issue. RSA's annual event always draws visionaries and well-known speakers from around the world and this year was no exception. The event attracted more than 35,000 attendees, over 500 exhibitors, up from 400 a year ago, and an audience with generally upbeat attitudes and very optimistic outlooks, well knowing that hacking, malware, ransomware, and cyber break-ins will continue to pester the IT world.

RSA President Amit Yoran's Opening Keynote

Amit in his keynote speech "Escaping Security's Dark Ages" said "The security industry is failing," later adding "It has failed." His main complaint was industry's lack of understanding. Organizations spot a breach and rush to clean it up before fully understanding the extent of the compromise. "We need to stop thinking of taller castle walls and deeper moats," he says. Complex passageways and nifty windows won't work either—no matter how high one builds or how deep one digs, attackers will still get through. "At the end of the day, even if you use next generation protective measures, focused adversaries with the resources, with the time, with the skill, and that have a defined objective of breaking into your organization are still going to get in," he says.

Internet of Things

The IoT buzz was everywhere—from Home Automation, M2M, to Smart Cities—but unfortunately very few speakers addressed associated security (or lack thereof) issues.

Discussing Smart Cities initiatives, Cesar Cerrudo, CTO, IOActive Labs, demonstrated how 200,000 traffic control sensors installed in major hubs like Washington; New York; New Jersey; San Francisco; Seattle; Lyon, France; and Melbourne, Australia, were vulnerable to attack. He has found ways to make red or green traffic lights stay red or green, tweak electronic speed limit signs, or mess with ramp meters to send cars onto the freeway all at once.

David Jacoby, Kaspersky Lab, exposed the inherent insecurity in home networks. He sends you a link to a new You Tube posting. You innocently click on it from your smartphone or tablet not knowing the link has an embedded JavaScript that runs on your device and detects all the devices in your home Wi-Fi network. The rest is easy; he can attack your router and you are compromised.

The problem, especially in the consumer Home Automation space is that security is not considered, understood and if it is, it is often an afterthought and bolted on using point solutions, antivirus, malware, OS cleaners. In this regard, initiatives such as BuildITSecure.ly are a welcome relief.

Services

Implementing IT security in any organization is highly Services-intensive. In fact, industry analysts report that for every $1 spent on hardware products, organizations spend anywhere from $3 to $6 on Services. This should be no different on security products. With this perspective it was no wonder seeing so many vendors emphasizing the Services aspect of their offerings. Accuvant and the traditional systems integrators Accenture, E&Y, and PWC are all focused on Services. Dell claims its Secureworks revenue is growing rapidly. FireEye has gained huge credibility and visibility after its acquisition of Mandiant and exposing Chinese hackers target 21 European foreign ministries, Southeast nations, India, and the U. S. HP offers cybersecurity solutions backed by professional and managed services and infosec architectures, frameworks, partners, and products. Pure-play managed vendors include Okta, Ping Identity, Proofpoint and Zscaler. Symantec is getting back to its core competency by trying to spin off Veritas soon, if it finds the right buyer offering the right price.

Data Center Security

This was probably one of the most talked-about topics in the Conference.

With the trend toward building large, cloud-scale mega data centers, organizations need to harden their physical and virtual servers as well as their private clouds; continuously monitor the security and compliance posture of their on-premise data centers, public clouds, and private clouds; protect legacy infrastructure from zero-day threats and new vulnerabilities, securely transition into software-defined data centers; and enable micro-segmentation to deliver application-centric security.

Workloads are moving across private, public, and hybrid clouds (e. g., Cisco Intercloud) and this trend is adversative to traditional network security controls, breaking traditional administrative policies and procedures. Vendors are weaving their stories based on their core strengths. Cisco, for instance, is marrying network security with ACI. VMware, with support from partners such as Check Point and Palo Alto Networks, is gaining market share with its NSX virtualization platform. With software-everything becoming a buzz phrase, vendors like Illumio and vArmour are pushing soft-defined approaches for heterogeneous cloud computing. Tufin is peddling a network security automation and orchestration solution. Realizing that any software-defined thing requires hardware to run it on, Juniper introduced a 2 Tbps version of its SRX firewall.

Enterprise Visibility

While some network equipment vendors are focusing heavily on network monitoring, analytics, DPI, etc., what is needed is visibility into an organization's *entire* infrastructure. There are many vendors offering products to gain better visibility of everything on the network:

- **Endpoint forensics**: Carbon Black, Guidance Software, RSA Enterprise Compromise Assessment Tool
- **Endpoint profiling**: ForeScout, Great Bay Software, Promisec, Tanium
- **Network forensics**: Blue Coat/Solera, Click Security, FireEye, WildPackets
- **All of the above**: IBM, Intel Security, LogRhythm, Splunk, Symantec

Legal Issues in Cloud Computing Security

Cloud Computing is a mishmash of multiple players—server, storage, network gear, and software vendors, cloud service providers, systems integrators, cloud service brokers, VARs…In such a complex scenario who is ultimately responsible for security, QoS, and SLA and who would you sue if the cloud is hacked or crashes? (If you are a Trial Lawyer, you'll sue everyone in sight!)

If you had a security breach in the cloud, **in the U. S.** many entities may hold you accountable, e. g., the FTC, the CFPB, Department of Health and Human Resources, U. S. Senate and House of Representatives, the SEC, State Attorneys General, to name a few.

Scenario 1: Your business is using a 3rd-party cloud app supporting your main product, and it holds customer data. It appears to have leaked customer data.

What do you do?

- What does the contract say? Any remedies or protections or requirements?
  - Investigation, response (including communications), notice to customers, duty to collaborate
  - Are you indemnified for this incident by the 3rd party?
- Do you have the ability to investigate directly versus dependency on application provider to investigate?
  - Asserting Attorney-Client Privilege in the investigation
  - Do you need to pull in outside assistance (technical, legal) to aid in the investigation?
  - If there are other app customers impacted, is there information that can be shared that would aid your response?
- Is the 3rd-party app provider managing PR adequately? Are the 3rd-party's statements adding to your legal risks?
- Is this event material?
  - What is the financial impact?
  - Customer impact?
  - Impact to your branding?
  - Does it trigger SEC reporting?
  - Have you notified your Board?
- Do you need or want to contact law enforcement?
- Probably for the first time, your marketing and branding teams will want to respond using social media to protect the brand, maybe even prior to the completion of the breach assessment. How do you intend to handle this?

Scenario 2: Compromise of the cloud service provider, potential impact to customer data.

What do you do?

- What does the contract say? Any remedies or protections or requirements?
  - Investigation, response (including communications), notice to customers, duty to collaborate
  - What audit rights do you have?
  - Are you comfortable with the adequacy of the CSP's compliance capabilities?
- Do you have the ability to investigate directly versus dependency on app provider to investigate?
  - Asserting Attorney Client Privilege in the investigation
  - Do you need to pull in outside assistance (technical, legal) to aid in the investigation?
  - Is the cloud service provider managing PR adequately?
  - Is this event material? Does it trigger SEC reporting? Have you notified your Board?
  - Do you need or want to contact law enforcement?
- CSP is preparing for class action, government inquiries, major media issues – what do you need as the customer to manage your legal risks?

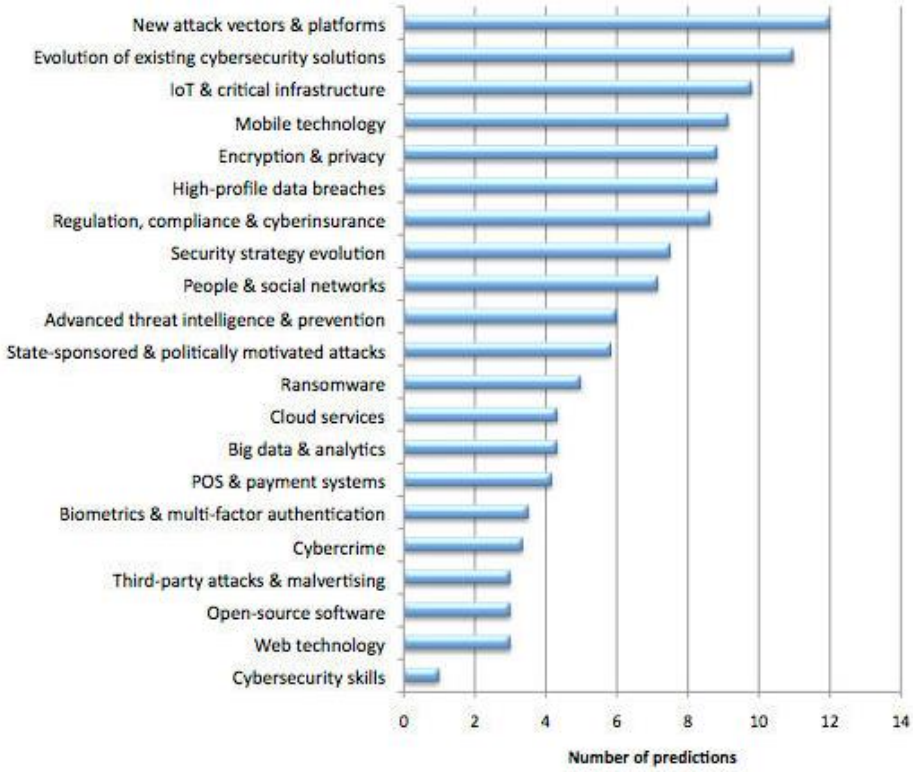
Scenario 3: Developing Apps for the Cloud.

- Standards and Best Practices matter a lot:
  - Are there standards or best practices must follow for development on a particular platform or for a particular service?
  - Are you using relevant laws or standards to help manage your customers' risks, to make your app more attractive for them?
  - Are there other relevant global standards or certifications that help mitigate downstream risks? (i.e., ISO 27034)

- What do the terms of the App store or sales platform for your app? Do they talk to security or your obligations in development or in an incident?
- Things to consider when you are developing:
  - Do you have an incident response plan? Does it include legal and PR?
  - What forensic capabilities do you have?
  - How secure is your infrastructure?
  - What promises can or should you make in your EULA?

What the future holds

Major security breaches in 2014 exposed almost 119 million records, not including the Sony Pictures Entertainment breach. The year 2015 doesn't look any better. The graphic below summarizes 2015 cybersecurity predictions.



2015 Cybersecurity Predictions

Security predictions from: Blue Coat, Damballa, FireEye, Fortinet, Forrester, Gartner, IDC, ImmuniWeb, Kaspersky Lab, Lancope, McAfee, Neohapsis, Sophos, Symantec, Trend Micro, Varonis Systems, Websense.

Hackers are always a step ahead of security professionals by the very nature of their activities and have developed methods to evade sandboxing techniques and divert investigators by "throwing more red herrings into their attacks to thwart investigators and intentionally planting evidence that points to an unassociated attacker," says Fortinet.

Hackers have already attacked, or at least demonstrated, cars' OBD (On-board Diagnostics) systems, cardiac pacemakers, kidney dialysis machines, defibrillators, insulin pumps, and baby monitoring devices. Gartner

predicted back in 2010 “By 2015, a G20 nation's critical infrastructure will be disrupted and damaged by online sabotage.” We have 8 more months to see if this prediction will come true.

Wrap up

On a personal note, we thoroughly enjoyed this year’s event, perhaps more so than in a couple of years. The event was very well organized and the Press was treated very professionally, with excellent working facilities, free Wi-Fi, and great food. The crowds were large and enjoyable. Among others, we stopped by LogRhythm’s booth to talk with some of their team, simply because they were so enthusiastic about their company and its team. The presentations were well attended and it appeared that there were a lot of behind-the-scenes negotiating among clients, prospects, and vendors.

San Francisco was up to its usual antics – the venerable Moscone Center was comfortable, but of course, there was the requisite closure of 4th Street, making it extremely difficult to move around.

Oh well.

We’ll be there, hope to see you at RSA 2016.

