Messages from the Front Lines: Pizzo, Cavoukian and Brown at SecTor2015

Rita Fundner 10 hours ago | Comments (0)

Messages from the Front Lines: Pizzo, Cavoukian and Brown at SecTor2015

Joe Pizzo's talk at SecTor2015, variously billed as "Data Driven Threat Intelligence" and "Ground Zero Financial Services: Targeted Attacks from the Darknet", reinforced the basic message highlighted by many others – speakers and attendees alike - that today's security world is a mess. Security has stopped working while the Darknet is experiencing exponential growth.

In a brief post-session chat, he confirmed that we're now, metaphorically, in a world that mirrors health conditions in the early part of the 20th Century, the pre-antibiotic era. Population numbers then were exploding, both cities and poverty were growing and wars and the usual diseases were slaughtering vast numbers but the best that could be managed by health professionals at the time was basic hygiene and skilled one-on-one care….a painfully slow and too-often, too-late, too-expensive intervention.

Corporations continue to vote with their wallets preferring to throw money at whatever went wrong after the fact. Writing off losses rather than investing in prevention actually makes good business sense when we all know there is no magic pill or process to prevent infection, effectively defend against attacks or even reduce their likelihood by any significant margin.

The lofty and laudable notion of privacy (and security) by design championed by Dr. Ann Cavoukian at her keynote talk "Security is Essential to Privacy – But it is not enough…Enter Privacy by Design" is a case in point. We have already, as an industry and long ago, embraced the notion that security, along with privacy should be baked into a product/service rather than painted on after the fact. It is a best practice that few decision-makers, builders or makers have actually implemented. Why? Because the innovation lifecycle, the time to market imperative and even agile methodology in the project world (among many other things) mitigate against it.

We all know, secretly, that building in security (much less privacy) is, at some level, while still the best we can do also a waste of time and resources plus a hated 'up

front cost. Most CSOs have discovered that you can get something from the business to combat sexy 'cybersecurity', less to address 'security' per say and not a penny to address 'privacy'. The business has learned that they need to be prepared to pay after the fact. Interestingly, the consequences of a privacy breach are less than catastrophic while service interruption costs big time and infrastructure meltdowns can kill the business dead.

Something that wasn't part of the original design is likely to come out of left field and need immediate, after the fact, crisis mode attention anyway… which is not to say security folks won't keep trying. They continue to hack away at bad guys with blunt tools all day long but currently the means to do a great job, a timely job much less a proactive job just don't exist.

Getting in front of the nasty beastie is where security needs to be and it's a daunting assignment illustrated by Jason Brown's talk on "The Globalization of Cybercrime" which showcased rearguard actions on an international stage. It was just plain depressing to hear how it takes months and years and an outrageous resource investment to set up sting operations that nab maybe one or two Darknet players….when an average attack cycle can be as short as ten days and less than 1 in a hundred are even detected. The biggest learnings from that talk

- Taking vacations abroad can be dangerous for criminals (sting) as well as CEOs (email takeover – more encryption needed!)
- The Nigerians are still out there doing their 419 idiot scams though the former Russian block and Middle East are stepping up their presence
- Don't bother paying anyone to ransom your device if some cryptolocker has it in a vice grip. Write it off. Best defence: off-site, off-line local backups.
- information sharing among law enforcement agencies is pretty pitiful given the layers of law: local, national and international
- the 2014 Data Breach Investigation Report may be useful http://asra.arc.nasa.gov/

So – what do we do in the interim on this still greenish planet?
Pizzo's advice in a nutshell:

. **to millennials & teens**: encrypt, use TOR, backup everything, and build your own solution! And read M.Sikonsk & A. Honig's "Practical Malware Analysis: A Hands-on Guide to dissecting Malicious Software"

. **to forensic investigators**: create bigger honeypots, focus on behavioral analysis, and focus on useful information (not every detail) meaning you'll never get any result going down every rabbit hole so figure out source and destination. Location in space/time is the context.

. **to the general public**: stop sharing USBs, stop clicking on the first item that pops up in a search, stop using modems and landlines. What are you thinking???? If you see something, say something!

Warm regards!!!

Comment on this article

Leave a Comment

☐ Connect to this blog to be notified of new entries.

Name | Your email address | PREVIEW | SUBMIT

You are not logged in.

- Sign In to post unmoderated comments.
- Join the community to create your free profile today.

Want to read more from Rita Fundner? Check out the **blog archive**.

Keyword Tags: security privacy SecTor2015 cybersecurity Darknet

Browse all IT Blogs