



Scott Crawford

RiskRecon: Navigating Security and Risk



SCOTT'S HOME EMA BLOGS HOME SCOTT ON VIDEO



posted by [Scott Crawford](#) | February 22, 2011 | one Comments

First of all, let me get one agenda item out of the way: What I [expected](#) to see at [RSA](#) this past week, I saw. Sadly, there wasn't too much in the way of news – but I did see a few things that, perhaps paradoxically, relate to last week's other high-visibility story in the IT world.

10 tweets
retweet



If you've been unconscious for the last several days, you are one of the 2 or 3 people in IT who doesn't know that, even though Ken Jennings gave the machine a run for its money on the final day, IBM's deep analytics and natural language processing engine known as "[Watson](#)" defeated the human champions of the game *Jeopardy!* Like many, I too am certain there will be application of this technology to security – even though there is clearly still a long way to go on the way toward true machine intelligence, if we ever achieve it at all.

Some have suggested that an approach such as Watson would be limited in its applicability to IT security. Computers are very good at solving finite set problems, particularly when the set is very large, but they may not be so good at things such as fraud, which poses an infinite problem set – or so some assert, at least as I understand it. I don't agree with this entirely. For one thing, fraud isn't so open-ended, at least in terms of its objective. Something tangible is usually at stake – like access to money, for example, or to valuable intellectual property. Even chaos can an objective, if the right targets are exploited. These can all be defined – at least in principle.

Where the problem is indeed more open-ended is that, in the real world, this definition can be difficult, to say the least. Objectives aren't always apparent. The value of assets at risk cannot always be measured directly. Harder still to grasp are the variety of ways in which access to an objective can be obtained or exploited. Add to this the many ways in which complex IT environments constantly change – not to mention that they interact with people – and one is faced with a set of variables that are difficult to incorporate at best.

But this is exactly why I think we need to consider the value of innovation such as Watson. Though I'm not a believer in silver bullets, I feel regardless that security would benefit from Watson's deep and fast retrieval of data coupled with an understanding of how humans seek a specific object – two fundamentals that directly address the complexity of interactions between people and technology that expose us to risk. And going a step farther: could such capability be put to work in a more dynamic approach to gamesmanship – which, after all, is one of the hallmarks of security – we may be able to deploy countermeasures that raise the challenge for the attacker above the static, predictable defenses (if any) that are the Maginot Lines of IT today (assuming that security [automation](#) itself can make similar leaps ahead).

I saw a bit of foreshadowing of this potential at RSA, among the more interesting vendor offerings at the event. [Mykonos](#), for example, "seasons" the HTML of Web applications that end users see with feints that engage the attacker and help to expose malicious behavior. The challenges of knowing whether or not such techniques were at play could conceivably help move attacks away from such "landmined" applications and toward targets where the risk to the attacker would be less. Of course, gamesmanship would enter into this as well at some point, as attackers seek to gain an advantage over such techniques – but this is where systems that understand this sort of interaction and respond accordingly might help to keep the bar high.

Needless to say, such systems are likely still far in the future – but I sometimes wonder just how far away they really may be. Are the objectives of attackers and the potential range of tactics truly so limitless? Or are there some constraints that would make the actionable understanding of IT risk more achievable at some

Subscribe to the RSS feed for Scott Crawford



- [Apple](#) [BI](#) [big data](#) [CCM](#) [Change management](#) [Cloud](#) [Cloud computing](#) [Converged Network Security](#)
- [Data-driven security](#)
- [data breach](#) [Dell](#) [EMC Corporation](#) [Firewalls](#) [Hadoop](#) [Hardware virtualization](#) [HCIA](#) [IBM](#) [IDS](#) [Information security](#) [Intel](#) [intelligence](#) [Intrusion Detection Systems](#) [Intrusion Prevention Systems](#) [IT risk](#) [McAfee](#) [Mobile](#) [Network security](#) [New School](#) [Next-generation firewalls](#) [PDCA](#) [Privacy](#)
- [risk management](#) [RSA](#) [breach](#) [RSA Conference](#) [RSA Security](#) [SecurID](#) [Security](#) [Security as a Service](#) [Security management](#) [Trends](#) [Unified Threat Management](#) [Verizon](#) [Virtualization](#) [visibility](#) [Zettaset](#)

FOLLOW ME ON [twitter](#)

[@nsselby](#) Still the Gummint, after all ;) [2011/12/11](#)

[@nsselby](#) Just saw it myself (via the Sporty's app). Guess they had to balance that G-rated sequence with SATAN as the other IAF... [2011/12/11](#)

...and IDEED is the missed approach fix if unable to land [2011/12/11](#)

point? Although many disagree, rational choice theorists such as [Bruce Bueno de Mesquita](#) suggest that some seemingly random outcomes may be more predictable than many think. Can such disciplines be successfully applied to the challenges of IT security?

Perhaps...but in the mean time, we still have much to do just to get a handle on what we already *know* we need to do better.

Related articles

- [What is Watson? IBM Watson and the DeepQA Project](#) (ibm.com)
- [By Request: We Are the IBM Research Team that Developed Watson. Ask Us Anything.](#) (reddit.com)
- [How IBM's Watson will make money](#) (cosmiclog.msnbc.msn.com)
- [IBM's Watson Win Poses Questions on What Is Next](#) (eweek.com)
- [IBM to Design and Build Advanced Cyber Security Analytics System for the FAA](#) (ibm.com)



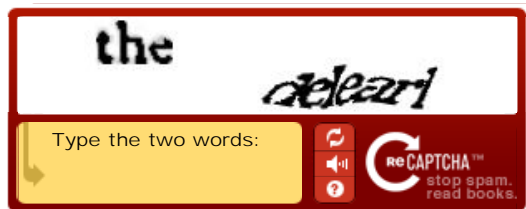
Posted in [Security](#) Tags: [Data-driven security](#), [IBM](#), [Mykonos Software](#), [RSA Conference](#), [Watson](#)

Pingback: [Tweets that mention RSA, IBM Watson, and the Future of "Smart" Security « Scott Crawford -- Topsy.com](#)

Your email address will not be published. Required fields are marked *

Name *
Email *
Website
Comment

You may use these [HTML](#) tags and attributes: `` `<abbr title="">` `<acronym title="">` `` `<blockquote cite="">` `<cite>` `<code>` `<del datetime="">` `` `<i>` `<q cite="">` `<strike>` ``



Just learned that the instrument fixes for the GPS approach to Runway 16 at Portsmouth, NH are (in this order) ITAWT, ITAWA, PUDYE, TTATT
[2011/12/11](#)

.@ashimmy on open-sourcing WebOS:
<http://t.co/aYRMzB4D> <The guy who called it back in August [2011/12/09](#)

[1 Raindrop](#)

[Amrit Williams Blog](#)

[Cognitive Dissidents](#)

[Krebs on Security](#)

[Layer 8](#)

[Open Group](#)

[Rational Survivability](#)

[RealGeneKim](#)

[SecAnalysis](#)

[TaoSecurity](#)

[The New School of Information Security](#)

[Threatpost Blogs](#)

[Verizon Business Security Blog](#)

[December 2011](#)

[November 2011](#)

[October 2011](#)

[August 2011](#)

[July 2011](#)

[June 2011](#)

[May 2011](#)

[April 2011](#)

[March 2011](#)

[February 2011](#)

[January 2011](#)

[December 2010](#)

[November 2010](#)

[August 2010](#)

[IBM Gives Industry Analysts Glimpse of the Future: How Will They Meet the Challenges Ahead?](#)

[Giving Thanks for Live Videoconferencing?](#)

[Fall 2011 WAN Opt Update](#)

[Thoma Bravo acquires Blue Coat: Initial Thoughts](#)

[APM and BSM – Evolution, Confusion and Business Ownership](#)



Shawn Rogers



Julie Craig



Charles Betz



Dennis Drogseth



Jim Frey



Dan Twing



John Myers



Gary MacFadden



Torsten Volk



Steve Brasen

© 2009 WP-1-STOP . All Rights Reserved.

[Pohl Media Studios](#)