Sleeper Awake

Amit Yoran

RSA Conference 2016 - March 1, 2016

I. Opening

A. We are all unique. We are each made up of a distinctive combination of genes, history, and environments, which results in each of us having our own individual perspectives. The experience of walking down a city street in San Francisco is different depending on whether someone is an artist who tends to view life through a prism of light and color, or an engineer that tends to focus on the structure and systems beneath life's façade, or a futurist who tends to view life not as it is but as it could be.

B. Our individual perspectives are very personal and unique to who we are. But, we're also influenced by the perspective of the world around us – the societies and communities in which we find or place ourselves. These communities shape our norms of behavior and create common experiences.

II. Review of 2015

A. Let's look at some of our common experiences from 2015. In February, we heard about the Anthem breach, the largest incident of PII theft to date.

B. Over the summer, we heard about what might be considered the most damaging breach in history; not just PII, or credit card data, but the most sensitive information you can imagine, information that truly defines you, information that could be used to target,

hurt, or blackmail people. 10's of millions of records. No, I'm not talking about the OPM breach. I'm, of course, talking about the Ashley Madison breach, whose tagline reads "life is short, have an affair." This proves that cyber is not only a booming career field, but that it can be a powerful conversation starter at home as well.

C. And just when we thought we had seen all of the humor our industry could offer, in September, the U.S. and China agreed not to hack each other for commercial advantage. Obviously, perspectives vary on the actual impact of the agreement. Rest assured, we're not cancelling the RSA Conference just yet. In fact this year's conference, our 25th, is the greatest one ever, by a long shot. We expect nearly 40,000 participants in attendance, and thousands more online, more than 500 vendors, and sessions from 700 plus speakers, thought leaders, and practitioners from around the world. And we'll even be joined by Jeff Spicoli!

D. Anyway, in December, Juniper Networks, one of the world's most reputable router companies, revealed that a backdoor had been inserted into its operating system unknowingly.

III. Our situation

A. Did any of these events really surprise us? If so, we haven't been paying attention.

1. The general purpose computing paradigm we operate under, cannot be secured. As a collection of complex, interconnected systems, our digital environments are at their core non-deterministic. This means that the infinite number of inputs and influences on our environments makes it *impossible* to

predict the universe of potential outcomes with any degree of certainty. And with the emergence of IoT, the problem is only going to get exponentially worse.

2. And yet, we continue pushing all of our communication, collaboration, and commerce online, pretending that our preventative technologies like anti-virus, malware sandboxing, firewalls and next generation firewalls, will keep us safe when we know they won't.

B. Intellectually, we get it. But that intellectual assent is not translating into changed behavior fast enough. RSA just completed a threat detection survey of 160 organizations around the world and discovered that 90% of respondents are not satisfied with the speed and capabilities they have in detecting incidents. Meanwhile, 2/3 of those organizations are still relying on a legacy perspective of SIEM for detection. Of course they're not satisfied.

C. My dad used to say, "You are how you behave," when trying to explain some gap between my intentions and my actions. I distinctly remember my *intention* was to clean the yard with my brothers but somehow we ended up accidentally setting the yard on fire (story for another time). Intellectually, you get that prevention is a failed strategy. That's a big step. But if you continue to invest solely in prevention, what good is "getting it?" Remember, "You are how you behave."

D. Gartner projects that by 2020, "60% of enterprise information security budgets will be allocated to rapid detection and response

approaches — up from less than 10% in 2014." Are you leading your organization into security's future, or still clinging to the past?

IV. A New Hope

A. The future is a new world order in which the technologies we deploy better align to the realities of our threat landscape. From this perspective, we need to emphasize monitoring and response, knowing that prevention will fail.

B. Today's modern computing environments leverage mobile platforms, cloud-based services, integrated digital supply chains, and dynamic employee and partner relationships. Authentication and Identity Management have come roaring back to the forefront of security conversations as the abuse of identity has become a key component of virtually every advanced attack, outpacing malware attacks as the most prevalent attack vector. I don't need to tell you that passwords have utterly failed. Even strong multifactor authentication needs the added perspective of fluid, contextual awareness. In addition to managing and strongly authenticating our identities, we need to monitor and govern them effectively.

C. But visibility into identities only takes us so far. We must push our visibility much deeper into our networks, our endpoints, and the cloud. Logs are simply not enough. We need visibility of full packet analysis of our networks combined with an understanding of telemetry from our endpoints to see exactly what is going on. At its very core, the key to security's future relies on

comprehensive visibility – getting and seeing the full picture. This is the base building block for obtaining truly insightful analytics and scoping out complex incidents correctly.

D. Speaking of which, behavioral analytics, AI, and machine learning will likely be all the rage during this year's RSA Conference and become part of our go forward buzzword bingo for years to come. I feel compelled to mention these advances for two reasons. First, because they hold great promise for enhancing how we do security. The second reason is rooted in a conversation I recently had with my future boss, Michael Dell. Following the announcement that Dell planned to acquire EMC, and by extension RSA, I had the opportunity to join Michael for dinner. After about 15 minutes of pleasantries, he turns to me and says, "Amit, I watched your keynote from RSA Conference last year. Would you like some constructive feedback?" To which, I replied, "Sure and I've been watching some of your speeches on YouTube and have some constructive feedback for you, too." Apparently, he agrees with some of my previous bosses on at least two things. I'm not as funny as I think I am and I definitely need a better grasp of the employer-employee relationship. Anyway, Michael explains to me that while I did a good job laying out the problems facing our industry, I failed to explicitly describe the solutions to those problems and tie such solutions to RSA's products. So to make my future employer happy, I'd like you to buy one of these, two of those, and a bunch of those over there. But in all seriousness, I am pretty excited that this week RSA is announcing the availability of

our own behavioral analytics platform, which is like Security Analytics magic, capable of detecting and highlighting incredibly sophisticated attacks never seen before. But while behavioral analytics and AI deliver incredible new tools for us to leverage, they aren't magic. All forms of analysis in a stovepipe, be they malware in a sandbox, end user behavior, or threat intelligence, can be readily bypassed, which is why pervasive visibility is foundational. No matter what any vendor claims, there is no actual magic that can save us. Consider the capabilities of state of the art AI – Google's AlphaGo system.

1. Just over a month ago, Google announced that AlphaGo, which combines advanced tree search with deep neural network systems has been able to definitively beat (5 games to 0) the reigning three-time European champion of China's ancient game of Go. For those that aren't familiar with Go, its a uniquely complex game with more than . . . well, a huuuuge number of possible positions; significantly more than the number of atoms in the universe. As impressive as that is, let me explain why AI will continue to struggle trying to master something infinitely more complex, like security.
2. While we might view advances like AlphaGo beating a human as proof that AI has advanced beyond humanity, games like Go, take place in a finite universe (a Go board), with extremely well-defined boundaries (the rules of the game). And most critically, all players - human and machine - must follow a constant and well defined set of unchanging rules. That's

pretty much the case for all successful applications of AI technologies: knowable, static rules that can be modeled for relevant lengths of time, with everyone playing by those rules.

V. Thinking about the "game" of cybersecurity, our opponent isn't playing the same game and certainly isn't following the same rules. In fact, our opponents don't really have rules. So in real life, who is sitting across from us at our gameboard? If we could unveil our opponents we would likely see incredibly creative human beings who are actively seeking to both understand and then subvert those statistical models themselves. Our continued belief that we can find a logical, repeatable set of rules by which we can play the game has resulted in the ongoing litany of breaches.Focus on the real issue

   A. For some perspective on tackling the cybersecurity challenge, let's take a step back and come at our problem from a different angle. Our problem is not a technology problem. Our adversaries aren't beating us because they have better technology. They're beating us because they are being more creative and patient and persistent. They are single-minded. They have a target – no prescribed path to get there, no overarching rules, just a target – and a virtually limitless number of pathways to explore.
   B. So how can we keep up, knowing that even state of the art analytics will be insufficient in the face of creative adversaries? What is the solution? Simple, we leverage our own smart creatives – our own curious, problem-solving analysts and set them loose to track down and hunt for our opponents.

C. Now before you say, “Hey, Amit, in case you haven’t heard, there’s a scarcity of talent out there - we can’t find or hire enough smart creatives,” let me tell you the same thing I tell my children. Stop whining!

1. If you don’t have hunters, grow them, or at least don’t stand in their way. Let them evolve into the hunters you need.
2. People are naturally curious. My daughter’s favorite word at five was, “Why?” Why, why, why? Free your people to chase the why. Allow, train, and equip your people to be hunters. Focus on empowering them with the tools that can fuel their curiosity and enable them to find the answers they seek.
3. Let me give you an example of growing your talent. Our Incident Response team was working with a large enterprise in the tech sector, who was owned, like, for over a year owned. RSA scoped the incident and cleaned things up, but like any organization facing a persistent adversary, ongoing monitoring and analysis would be required. One of our IR folks teamed up with one of their internal analysts, trained him, and had him shadow our activities, making sure he understood the methodology and process of hunting. Over the course of a few months, he became a master analyst, capable of hunting on his own, actively combating sophisticated threat actors interactively, denying them access to systems which would otherwise remain owned for months or years.

D. You can do this, too.

VI. Creating heroes

A. Create a culture that embraces the free thinker, the curious. If your security program is focused first and foremost on compliance, then you're doing it wrong. Embrace the freedom to actively hunt for adversaries, you'll attract the right team, and in doing so, create the right culture.
B. Companies also need to focus their investments on technologies that enhance rather than replace human creativity and problem solving. Technologies that automate routine and mundane tasks help. Black boxes that just throw off alerts without supporting data or explanations provide the illusion of security. We need to know *why* something is being flagged. We need tools that give us the comprehensive visibility we discussed earlier; the perspective to see the whole playing field and when rules are being violated.
C. But the private sector can't do this alone. We need the government to enact policies that help rather than hinder security. Providing opportunities for talent development by incenting education? Awesome.
    1. However, we frequently see governments muddying the waters by allowing intelligence communities or law enforcement to dominate national cybersecurity policy and initiatives. Their perspective and agenda differs greatly from those trying to defend networks.
    2. Some policy proposals, like weakening encryption, are so misguided they simply boggle the mind. In an era where cyber is consistently cited as the single greatest threat to our way of life, above terrorism and all else, how can we justify a policy

that would catastrophically weaken our infrastructures? Contrary to the going dark rhetoric, we live in a golden age of surveillance, more so than at any other point in history. Weakening encryption is solely for the ease and convenience of law enforcement in going after petty criminals. No credible terrorist or foreign intelligence service would ever use technology that was knowingly weakened. However, if we weaken our encryption you can sure bet that the bad guys will exploit it. Such a policy would harm US economic interests on an already suspicious world stage, as well as unconscionably undermine those trying to defend our digital environments in every industry.

3. At this time I'd like to recognize and thank a number of players who's presence here at the RSA Conference symbolizes a sincere effort to build a stronger relationship between the government and private sectors. Joining us this year we have the director of the NSA, a number of national cyber czars, members of Congress and Governors. I am especially appreciative that the Director of the FBI and the Attorney General of the United States will join us and engage with the security community at RSA this week. It means a lot. We need to be respectful, but we must also make sure our voices in this debate are heard loud and clear.
4. And finally, let me mention the many accomplishments of the Department of Commerce in cyber, including updating the privacy framework enabling better cooperation between the

EU and the US, the soon to be updated NIST Cybersecurity Framework that is being adopted internationally, and the many definition languages that allow us to build interoperable tools. That said, the Obama Administration's inclusion of cybersecurity technologies in the Wassenaar Arrangement is, to put it charitably, absurd. For those of you who aren't familiar with it, the Wassenaar Arrangement is designed to prevent the spread of technology for offensive use, to evil and oppressive regimes. It is conceivable that offensive tools and exploit kits might warrant some restriction. And while monitoring platforms might be perverted or used for bad purposes, the answer cannot be to deny their efficient use to all organizations trying to defend themselves. The misguided current interpretation effectively criminalizes every company trying to monitor their global digital infrastructure against cyber threats and doesn't practically solve any problem.

5. The private and public sectors need to think differently.

VII. Wake up

A. Some of my favorite vacations over the years have been the ones with my brother in which we push the envelope – "death wish" adventure vacations on glaciers in Iceland, running with the bulls in Pamplona, dog sledding, or winding through mountain passes on motorcycles. There is a certain thrill in planning out a challenging trip and then relying on our wits and stamina to come out on the other side successfully with an amazing experience. Security is not for the faint of heart either. The cyber-world is a

dangerous place, but not one that can be avoided. If we are going to survive we need to follow the same process of planning and preparation. What are the right products to buy? Who are the right people to learn from and lean on? How do we train hunters and create the culture we need to be successful?

B. Our industry was founded and built by mischievously creative, almost eccentric, pioneering "renegades." We celebrated the diverse perspectives of the artists, architects, and geeks. Nonconformists. People that thought differently. Art history majors, physicists, a bee keeper, and maybe a few mathematicians like these guys in the front row. Let's reclaim our heritage of intellectual curiosity, and rekindle that crazy, creative spirit that brings diverse perspectives.
C. Remember, you are how you behave. Our industry needs to wake up. So, what are *you* going to do differently this year?