RSA PRESIDENT AMIT YORAN KEYNOTE ADDRESS AT RSA CONFERENCE ASIA PACIFIC & JAPAN

July 22, 2015

Singapore

We are a world of diverse nationalities, religions, ethnicities and languages. They define us – give us meaning, and provide us with an identity. Young. Old. Man, woman and child. Given our uniqueness in the physical world, it is ironic that our identity is such a slippery concept in the virtual world. While a fingerprint, voice pattern or retinal scan uniquely identifies our physical identity, our virtual identity is defined by a user name and password. Leading us to wonder – in this virtual world -- are you really who you say you are? Are you an imposter? Can I trust you?

For the sake of unlocking the potential of our shared digital world, those are questions we had better come to terms with.

Ladies and gentlemen, yes, *I'm* Amit Yoran. There's no denying that. I've got a conference credential with my name on it, just like you. And my black shirt has a little red "RSA" logo down here somewhere. There! Authenticated!

In this venue, your conference badge tells everyone who you are. And what sessions you have access to. Yet for today's businesses, tasked with managing digital resources…delivered on premise and in the cloud…accessed from corporate networks as well as mobile devices …by hundreds and thousands of employees and partners, figuring out who's who and giving them access to what they're *supposed* to have access to, isn't quite as clear cut…especially while trying to keep the *wrong* people out.

I'll come back to that in just a bit.

The fact is, most organizations still don't really understand the severity and the complexity of the threat landscape we are facing today. While the turnout this year for RSA Singapore is a record, even a brief review of the news over the past few years shows we have far to go.

The largest enterprises with the most sophisticated, "next-generation" security tools have not been able to stop the bad guys from making off with millions of dollars, extensive personal information, confidential M+A documents and countless other secrets.

The past few weeks alone have brought some pretty shocking revelations. In America, a site has recently been hacked which contained some of the most sensitive information of more than 20 million Americans. The information could cause great personal embarrassment and make them subject to blackmail and social engineering.

But no, I'm not referring to the devastating attacks suffered by OPM [Office of Personnel Management]. I'm talking about the really sensitive information on Ashley Madison. For those of you who don't know, Ashley Madison is a site for cheating spouses. Their tag line is "Life is short, have an affair."

This proves that cyber is not only a booming career field, it's a conversation starter at home too.

Please remember as the data from Ashley Madison comes out, you should ignore any of the sexual proclivities of the handle “Deep Panda.”

OK, back to the matter at hand.

Clearly our adversaries are out-maneuvering and outgunning the security industry, and winning by every possible measure. Once inside an enterprise’s network, they often go undetected for months or even years. The only way forward is to change our cybersecurity mindset.

Whether self-delusion, ignorance, or marketing from security vendors, it doesn’t matter. Quite frankly, legacy mindsets in security display negligence, if not insanity.

The misguided notion is that prevention will keep the bad guys out. It won’t. Don’t get me wrong, next generation firewalls, anti-malware technologies, and the rest are all nice to have, but if you believe for one second they’ll keep the bad guys out of your environment, you’re asleep at the wheel.

Changing your mindset is hard. I get that. Yet history has demonstrated time and again, when facing a new era of challenges with old era thinking, it never ends well. So trust me, not changing is much harder, or at least comes at a much greater cost.

Let me give you an example of an enterprise that gets it. Don’t laugh. It’s your friendly, local post office. For too long it was a place to stand in line and wait to be acknowledged by someone behind the counter. Then you’d wait for your package to be weighed and stamped. And then do it all over again. How old school is that? I mean, who mails letters anymore?

Postal services around the globe realized that they needed to evolve if they were going to be relevant, or even survive. A few miles from here, Singapore Post, the nearly 200-year-old national post service, is doing just that - reinventing itself as a modern day digital enterprise, transforming into a one-stop shop for retailers’ booming e-commerce needs across Asia.

Besides traditional services, SingPost offers website development, online marketing, and, of course, package delivery. Singapore’s central location makes it an obvious hub for e-commerce across Asia, with more than 600 million people living in the immediate area, and more than two billion people within a five-hour flight. That’s a quarter of the world’s population.

E-commerce now accounts for more than 25 percent of SingPost’s revenues.

Japan Post just bought the largest private package and freight delivery company in Australia, Toll Holdings. It has created a global rival to UPS and FedEx. Australia Post is working with Alibaba to help local businesses connect with Chinese customers.

These radical transformations are happening within our national postal services. Talk about an impressive shift in mindset.

Meanwhile, the security industry is still selling stamps.

In a world of sophisticated advanced threats, the security industry is still selling the perimeter as the primary line of defense. Beyond our irrational obsession with perimeter technologies, some of us still follow an equally absurd path to detecting advanced threats.

Monitoring is performed with signature-based intrusion detection systems and anti-malware products. It's not that perimeter and preventative measures are bad in and of themselves; it's that they are limited by experience. They have to have seen a threat before, or have been taught about it, in order to detect it. We all know that the threats that matter most today are the ones you *haven't* seen before. These tools are incapable of detecting these advanced threats…threats that cause the most damage.

Nonetheless, so many security professionals base their monitoring programs on the futile aggregation of telemetry from these virtually blind IDSes, AV platforms, and firewall logs, implementing that glorious and increasingly useless money-pit, known as the SIEM. It may have been a shock to them when last year's Verizon Data Breach Investigations Report asserted that less than one percent of successful advanced threat attacks were spotted by SIEM systems. Less than one percent.

The game has changed but so many are still clinging to selling the stamps we are so comfortable with.

So how do we re-program ourselves for success? What is the path forward? Let me share five thoughts on navigating the digital landscape, based on my conversations with CISOs, CIOs and my own experiences over the past two decades.

First. Let's stop believing that even advanced protections work. They do, but surely they fail also.

Here's the news flash that has underwritten each and every spectacular intrusion we read about on a daily basis and countless others that remain undiscovered and unreported – and that is that a well-resourced, creative, and focused adversary is going to get into your environment. Every modern nation-state and every organized criminal enterprise operates aggressive intelligence collection and monetization schemes online. They enjoy limitless bounty with near perfect impunity.

You'll see many promises made this week – expect to see more big data solutions, solutions to IoT, "fire and forget" analytics, and all sorts of other buzzwords, but challenge yourself and challenge us vendors does this really help or is it yet another castle wall that will inevitably be breached?

We're seeing analytics-resistant malware that can evade detection by sandboxes and other advanced systems. No matter how high or smart the walls, focused adversaries will find ways over, under, around, and through.

Second. We must adopt a deep and pervasive level of true visibility everywhere – from the endpoint to the network to the cloud – if we have any hope of being able to see the advanced threats that are increasingly today's norm. Consider Stuxnet, Equation Group, and Carbanak intrusion sets and countless other sophisticated campaigns. One of the defining characteristics across all of them is their stealthy nature.

Until written about, they were virtually undetectable because they bypassed traditional defenses. Even now, many organizations operate completely blind as to whether they are victims to these published techniques or not.

We need pervasive and true visibility into our enterprise environments. In reality, I'm describing now what SIEM was meant to be, or rather what it *should* be. You simply can't do security today without the visibility of both continuous full packet capture and endpoint compromise assessment visibility.

Within our networks, we need to know which systems are communicating with which, why, any related communications, their length, frequency & volume, and ultimately the content itself to determine what exactly is happening. These aren't nice-to-haves. They are fundamental core requirements for doing security today. If you don't have that level of visibility and agility in place, you're only pretending to do security.

Traditional forms of visibility are one-dimensional, yielding dangerously incomplete snapshots of an incident let alone any semblance of understanding an attack campaign.

Without the ability to rapidly knit together multiple perspectives of an attack, you'll never fully understand the scope and the overall campaign you're dealing with. Frequently, sophisticated adversaries are executing attacks using multiple tactics in concert, often from separate attack groups to assure persistent access.

The single most common and most catastrophic mistake made by security teams today is under scoping an incident and rushing to clean up compromised systems before understanding the broader campaign. In fact, let me say that again. The single greatest mistake made by security teams today is under-scoping incidents and rushing to clean up compromised systems before understanding the true scope of compromise and possibly broader campaign. Without fully understanding the attack, you're not only failing to get the adversary out of your networks, you're teaching them which attacks you are aware of and which ones they need to use to bypass your monitoring efforts.

And I'm not just standing up here and saying "buy RSA gear." I'm the first to admit that we need to go further than what is available today. We're on a journey to full visibility. Our environments, business practices, and adversaries continue to evolve, and so must we.

Third. In a world with no perimeter**s** and with fewer security anchor points, effective identity management matters more than ever. That boils down to three things – governance, access and lifecycle. Governance is *understanding* who should have access to what. Access is *controlling* who has access to that information. And lifecycle is *managing* the evolution of that access over time.

Identity must be managed past the gateway.

Traditionally, organizations have taken a Band-Aid approach by implementing point solutions and fixing problems where they exist. Single Sign On for here; a governance solution for there; a separate mobile device management solution for tablets and smart phones; provisioning for this and for that. That mindset has to stop.

Security will never succeed just being a cost center. We need to start taking a more holistic approach so that identity can become a strategic business enabler.

Here's what I mean. Stop being a gatekeeper and think business centric. Focus on achieving the goals of the enterprise. To be business centric, we need to involve business owners early and often. We need to give them control over the lifecycle and privileges of identities…giving the right people access to the systems, applications and data they need. It can be done.

Why am I emphasizing identity so much? Consider the evolution of today's threat actors. We tend to think about adversaries secretly developing vicious malware in a dark basement somewhere. That's our traditional view of the world. The reality is that malware is the primary attack vector *in less than half* of advanced threat breaches. Don't mistake an anti-malware solution for an advanced threat strategy.

In breaches where confidential data was disclosed, the most popular method used was the Web application attack. And in those cases, 95% of the time, attackers used stolen credentials and simply walked right in. The Verizon Data Breach Investigations report talks about how often user credentials , not sophisticated malware or hacks, open the gates to the adversaries.

At some point in every advanced threat campaign, the abuse of identity is a stepping stone the attackers use to impose their will. The creation of sysadmin or machine accounts, or the abuse of over-privileged and dormant accounts, facilitates lateral movement and access to targeted systems and information.

Strong authentication, and analyzing who is accessing what can identify attack campaigns earlier in the kill chain and make the difference between successful response and unmitigated disaster. Don't make the mistake of trusting the actions of the trusted; those privileged accounts and executive users are the ones most targeted, and are precisely the ones we should be most suspicious of.

Fourth. Intelligence. This is a core requirement today as well. According to the Security for Business Innovation Council, only 43% of organizations augment internal threat intelligence with external data. There are incredible sources for the right threat intelligence for your purposes, from private vendors and organizations like ISACs.

Just as important as external threat intelligence is internal threat intelligence. The CISOs that give their security teams time to hunt around the environment to understand what normal looks like will quickly spot unusual traffic patterns. In the same way a neighborhood police officer gets to know people, cars, and comings and goings in a neighborhood, so the unusual strikes him immediately as odd, so too can your analyst hunters – if they are given the time to do it.

Fifth and finally. Your security program needs to be guided by an understanding of risk. You must understand what matters to your business and what is mission critical. This asset categorization isn't the sexy part of security, at least not Deep Panda handle style, anyway.

But it is critical to helping you prioritize the deployment of limited security resources for the greatest possible impact. You have to focus on the important accounts, roles, data, systems, apps, **and** devices – and defend what's important and defend it with everything you have.

These five principles can work. They do work. We've seen the difference it makes when organizations take these approaches to security. We see customers understand the attack campaigns that have been running in their environment for months or longer - often right under the very noses of their intrusion detection systems and protective measures. In one incident response effort, we discovered breach artifacts that were in place for seven years. Seven years.

With these ideas and agile mindsets, our teams are even catching attackers red-handed, and disrupting their ability to exfiltrate data and achieve their objectives.

I'm not saying we have all of the answers. Far from it. There are resource challenges, skill gaps, and legal impediments. But we are on a path to changing a paradigm under which our industry has operated for decades. And at RSA, we're starting with ourselves. We're re-engineering RSA across the board to enable us to deliver on this vision. As an industry, we are on a journey that will continue to evolve in the years to come through the efforts of all of us.

I'm reminded of an old story from the age of exploration when many maps weren't yet complete. There were uncharted areas of our world. As the story goes, a captain was sailing his ship and reached the edge of his map. He sent word back to his commanders, "Have sailed off map. Am awaiting instruction."

In security, we find ourselves in uncharted waters. We have sailed off the map, my friends. Sitting here and awaiting instructions? Not an option! And neither is doing what we've been doing – continuing to sail on in these new waters with our existing maps. What I'm describing is not a technology problem. We have the technology today to provide true visibility.

Strong authentication and identity management solutions are readily accessible. We have great threat intelligence and insight into even sophisticated adversaries. And we have systems that map and manage our digital and business risk.

This is not a technology problem. This is a mindset problem.

The world has changed. We must change, too. I hope you use the conference to start thinking about that change. But remember, that change has to start right here.

Thank you.

# # #