RSA CONFERENCE EUROPE FINAL (10/28/13)
Art Coviello Keynote: October 29, 2013

Welcome to RSA Conference Europe. It's great to be in Amsterdam, the commercial capital of the Netherlands.

It is fitting that we are holding our conference in a country that was instrumental in igniting the explosive era of world trade in the 1600's that has evolved through the centuries leading to the creation of today's interdependent global economy – an explosion, by the way, based on a model combining innovations in Technology, Commerce and Political Philosophy.

In technology, the Dutch made advances in the design and construction of sailing ships giving them significant competitive advantage at sea. In commerce, they developed free market rules for trading commodities and the production of goods, as well as the efficient use of capital. The Dutch invented the stock market. All of which gave them economic advantage. And finally, in political philosophy, their oligarchic form of government sowed the seeds of an open political system that focused on the multitudes of its citizenry and not just the nobility.

But the Dutch don't live in the past.

Having lived through dynastic and religious wars, the Napoleonic Wars, the rising trade protectionism that developed in the 19th and 20th centuries, and the devastating World Wars, the Dutch continue to be at the forefront of economic prosperity.

With a rank of only 63rd in global population, the Dutch economy is 17th largest in the world. Only countries with significantly larger populations produce more.

There is a conference full of lessons to be gleaned from this history as today's world trade parallels that of the past with the innovations in sail and the use of sea lanes for communications and commerce replaced with innovations in Information Technology and the Internet.

In my keynote this morning, I'm going to focus on lessons we can learn that are relevant to our topic: security…. and related impediments to the ongoing expansion of technological innovation.

As trade flourished in the 17th century, a number of adversaries arose to compete with and inhibit trading by nations like the Netherlands, not unlike what we see in today's global economy.

The rivalry of nations still exists, as nations jealous of the economic advances of others plunder not cargo ships, but intellectual property and trade secrets.

Religious wars have been replaced by the actions of misguided religious fanatics, terrorists, who want to cause economic and physical harm.

We have our modern day pirates, the ecosystem of criminals, who, in the blink of an eye, can steal money or engage in credit card fraud, often from continents away – a lot easier than stealing treasure while sailing under the Jolly Roger.

And we have political turmoil, only this time not in the form of dynastic wars, but in the form of hacktivists bent on altering the political landscape to suit their ends.

But today's attackers have methods and goals that are ever more sophisticated and alarming. Intrusive attacks are being joined by disruptive attacks, which will ultimately lead to destructive attacks.

Yet there's another parallel. Just as, more and more nations began trading, leading to the use of more and more trade routes, creating more and more avenues of attack, today's attack surface is also expanding rapidly. Just look at how much our attack surface will expand over the rest of this decade.

Ten years ago we still ran our organizations on client/server applications. Today, Web apps predominate and by the end of this decade "Big Data" apps will be the real crown jewels. Intelligence derived from mining rich sources of data about all of us and the world around us will create advances in productivity and efficiency that lead to unparalleled value for us, but potentially for our adversaries as well.

There will be plenty of data for us and our adversaries to consume as we continue to accumulate it at an astonishing rate.

The way we access it will also expand the attack surface. In just seven years since the invention of the iPhone, we have full mobile ubiquity and by 2020, thanks to the implementation of IPv6, we will have not 1 billion devices connected to the Internet, but 200 billion, many such devices being part of critical infrastructure.

Personal information will also be part of the attack surface as we willingly give it up on social media sites and for vendors' loyalty program, unwittingly also giving our adversaries new avenues of attack that we have paved ourselves.

The result of all of this is our traditional methods of defense are increasingly ineffective.

The perimeter has disappeared. Physical infrastructure will be harder and harder to protect and traditional security controls are being obsoleted.

We are in danger of being overwhelmed by these changes to our environment, just as the Dutch trading empire was overwhelmed in the 18th and 19th centuries by wars and

protectionist trade measures in its international markets.

But history doesn't have to repeat itself. We can change. The good news is that we are changing.

Intelligence-Driven Security is being increasingly adopted by the industry and promises a radically different, much more effective model of security using Big Data thinking and technologies.

As shown here, Intelligence-Driven Security starts with a deeper understanding of risk – our key assets, vulnerabilities, potential attackers, and commensurate risk mitigation policies and compliance requirements.

In this model, more agile and dynamic controls that can react to facts and circumstances replace outdated perimeter ones. These controls will have their own analytic capability (intelligence) to detect and respond to attacks in a timely manner, preventing loss.

We are also revolutionizing security by adding *context* to the equation (again a form of intelligence). As you all know, context can make a big difference.

Existing controls are siloed and one-dimensional – they don't add value to one another.

I'm sure you are all familiar with the story of the blind men and the elephant. Each one touches a part of the elephant and can describe the feature accurately – a tusk, a trunk, a tail or a leg – but no one can accurately describe the whole elephant.

Today's controls are like the blind men trying to describe an attack or attacker to your Security Operations Center – providing data but never "seeing" the whole picture.

By integrating security controls, enabling them to interact with and inform each other, we are giving them context. By combining intelligence about potential attackers, network traffic and user behavior, we are adding even more context.

When we comprehensively understand the context or "normal" behavior of people and the flow of information on our networks, we are able to transcend reactive measures to more clearly and quickly spot even a faint signal of any impending attack or any intrusion, in the midst of an increasingly noisy environment.

This is what makes intelligence driven security future-proof. It eliminates the need for prior knowledge of the attacker or their methods. Because no matter how clever, sophisticated, stealthy, and well-resourced our adversaries are, at some point, these attackers, if they are going to gain any value from their actions, will have to do something anomalous. Criminals can masquerade as customers. Adversaries can compromise employee or partner credentials. But sooner or later, to achieve their goals, they need to do something out of the norm; something

your customer, partner or employee wouldn't do. And when they make that anomalous move, that's when we expose and stop them!

To gain this context, we are obviously going to have to get much better about how we make sense of our networks and the data flowing across them. We need our security systems to behave less like a police headquarters that responds to criminal incidences once they're called in and more like your neighborhood police officer.

The officer is out in the neighborhood and knows the comings and goings of the people and general flow of life. That context allows him to spot the unusual and, instead of reacting to crimes, be in a position to prevent them. Technology can even play a role, and here's an example. I'm particularly impressed by how the Netherlands is modernizing communications between police and citizens via Twitter – real-time insight and communication via a popular, modern medium.

We, in the security industry are getting there too. Tools have become available that provide neighborhood police levels of monitoring and context. My colleague, Amit Yoran, will be talking about them in a moment. But before he does, I want to address a serious complication in our ability to make progress in this regard. One that is very much in the news – privacy.

At last year's Conference, I pointed out the danger of an imbalance between privacy and security.

There are absolutely legitimate concerns about having network activity monitored at such a granular level. What about the privacy of those using the network? And this isn't just an academic debate – some of our customers are caught in an agonizing and paralyzing Catch-22, literally afraid to deploy technology that would protect theirs and their customers' privacy for fear of violating workers' privacy. Of course, that conundrum ignores the fact that the exact same technology would also protect those workers' privacy.

This demonstrates the consequence of pitting security against privacy. The reality is that security and privacy are like the two poles of a magnet. Misaligned they become opposing forces driving each other apart. Aligned, they attract each other, forming a powerful bond But if we want both security and privacy – and I'm telling you *we can* have both – we have to align the two in an environment that can be trusted.

Let me explain.

When sophisticated security tools like the ones I described are implemented objectively, dispassionately, and with strong governance, privacy is possible. In fact, that's the necessary outcome. But not only is that how privacy is possible, that's the *only* way privacy is still possible today, given the open, interconnected nature of our shared digital world.

With adversaries cutting apart our existing security defenses left and right, the only way we can

hope to protect the information that is most valuable to us is through understanding anomalous behavior of people, devices and the flow and use of data.

Nevertheless, this level of insight does have the potential to be misused.

We don't want to create Big Brother, which, ethics and morality aside, would stifle and eventually kill innovation. We must strike a balance between the extremes of an Orwellian oversight of the people using our networks and an equally dogmatic allegiance to anonymity, which is in reality the enemy of privacy.

Let me repeat that.

Anonymity is the enemy of privacy. An anonymous network gives free rein to our adversaries who want nothing more than to access and use or misuse our private data, with no risk of discovery or prosecution.

Balance is struck through the application of appropriate transparency, governance, and technology.

- Transparency - we must be transparent and above board with our monitoring processes, helping people to understand that we monitor our networks to ensure security and privacy.
- And Governance - we must establish strong protocols and technologies to enforce those protocols so that our actions are objective, dispassionate, and fully dedicated toward one end and one end alone – the security, integrity, and privacy of our networks and the data they transmit as well as the people using them.
- Finally, Technology can be used to anonymize certain data that can then be used in the pursuit of security when we don't actually need to know from whom or where the source is.

If we can strike that balance, through the application of Intelligence-Driven Security wrapped in transparency and good governance, then we will have the best of all possible worlds – the free or, should I say, the responsible flow of information.

I began my talk by discussing the Golden Age of the economy of the Netherlands, in which technological innovation and free trade created an economic boom that lifted its people's standard of living and made the country the envy of Europe, if not the world. But remember what brought it to an end – war and protectionist trade measures that choked off the life-blood of its economy.

Today, we live in the information era and our global economy is dependent on the responsible flow of information. If we do not integrate security and privacy and instead end up at either extreme, we will not have heeded the wisdom of George Santayana who said, "Those who don't learn from the past are condemned to repeat it."

We will choke off the critical flow and use of information, create our own protectionist measures, and still be at the mercy of criminals, hacktivists and rogue nations.

But we're not going to let that happen, are we?

We, in this industry, understand the technical challenges of the security/privacy debate better than anyone. It's up to us to lead. It's up to us to ensure we have an informed and civil discussion that leads to good policy and the right technical solutions.

Once again, the Dutch can be a shining example. Following the devastation of the Second World War, the Dutch were instrumental in architecting the common market that lead to the open flow of commerce in the EU today.

The common market was about nations overcoming their ancient rivalries. It was about synergy triumphing over perceived self-interest. It was about collaboration and compromise. That's the sort of thinking and innovation we need today.

Thank you.

Now I'd like to invite my friend and colleague, Amit Yoran, onto the stage to lay out in more detail how an Intelligence-Driven Security model works and specifically how it reunites security and privacy.

H12514