ASX ANNOUNCEMENT | COVATA LIMITED

Trent Telford

Cyber Security Summit NYC Transcript

(Full Presentation Available - https://www.covata.com/wp-content/uploads/2015/09/J3068_COV_Data-Centric-Presenttion_V3.2.pdf)

Keynote Address

Friday 18, September 2015

Thank you everyone.

I want to talk to everybody today, probably on a little different approach than others are talking about when it comes to security. That is talking about a data centric approach – protecting the data itself, and not just relying on network related tools to do it for you.

I want to show you the way we at Covata think about security and how our partners are approaching security.

[Slide Pg 3]

The first thing to remember is that the Internet wasn't designed to be secure; it was actually designed to share information. If we look at the history of the Internet and what its initial objectives were we begin to understand the thought process behind the "internet" architecture we largely use today.

In 1973 the US Defense Advanced Research Projects Agency (DARPA) initiated a research program to investigate techniques and technologies for interlinking packet networks of various kinds. The objective of the research team was to develop communication protocols, which would allow networked computers to communicate transparently. The project was called the "Internetting project" and the system of networks, which emerged from the research, was known as the "Internet."

[Slide Pg 4]

Fast forward nearly 20 years to 1991 and the Internet had grown to include some 5,000 networks in over three-dozen countries, being used by over 4,000,000 people. The underlying principle had not changed. The Internet was allowing the free flow of shared information.

Conscious that we only have an hour for lunch, let's fast forward again to today. Today there are 3.2 billion people using the Internet – which still only equates to 44% of the worlds population. Which means a staggering number of people are rapidly coming online.

As of last year there is over 1 billion websites on the Internet. Let's try and visualize just how much data all of these people and websites are creating - Think of it this way—five exabytes of content were created between the birth of the world and 2003. In 2013, 5 exabytes of content was created each day.

The stats clearly show that we have taken what the Internet was intended to do and aced it. The amount of things we have done, the amount of data we have created and shared, the amount of businesses and industries we have transformed thanks to the Internet is astronomical. Even 50 million Americans have the Internet to thank for their dating life. The problem is, however, that for all of the businesses, homes and people we have connected, we have also created end points through which data can be pilfered, stolen and used for nefarious acts.

[Slide Pg 5]

This quote from FBI Director Robert Mueller sums up the predicament we now find ourselves in. Because of how we have engineered the Internet and subsequently our businesses we are now all exposed to the world of cyber crime. Mueller said this in 2012, and I think it is fair to say we have seen more than enough evidence to support his statement.

We cannot blame ourselves entirely for the dramatic rise in large-scale hacks. The notion of security has weaved its way into boardroom conversations and businesses attempted to keep up with the latest security offering. For the first 20 years of the Internet we protected the perimeter. We attempted to lock down our businesses from the dangers of sharing cart blanche by using firewalls, gateways and secure connections.

[Slide Pg 6]

The best way to look at our historic approach to security is the analogy of our elderly grandmother coming into work and stitching together a solution for us. Using firewalls, gateways, secure tunnels as a mesh, she encases the business in a warm protective embrace of security. However, like anything that is knitted together there are holes and imperfections as grandma does her best to make the different strings bind together. Whilst a layered approach to security is important, you cannot stitch together a solution and hope that there are no holes. What we have here is a retrofitted approach to what has fundamentally been built as an open network. It does not work.

We have fought valiantly as business community to build higher walls and put in thicker pipes. Yet we have seen hackers build higher ladders and bust through thicker walls, breaking through the perimeter and procuring the crown jewels inside your organisation - and that is your data.

In recent years most people would say that the model of securing the perimeter is broken. When Richard Clarke, who we all probably know as the first cyber tsar of the Whitehouse came out and said it was broken, he said the Pentagon had been hacked, the Whitehouse has been hacked etc, and I think it is fair that we need to all start looking at it a bit differently.

[Slide Pg 7]

It almost feels like Groundhog Day, every day waking up to a new hack on a major institution or Government Agency. We probably all have a case of hack-fatigue, but considering I am encouraging you all to think about a data centric approach to security, let's look at some of the higher profile hacks that we have seen and understand what went wrong with their approach.

These companies and the incidents that I am about to refer to, have been publicly identified and reported. I think that to some extent we should have empathy for these companies. I would hasten to add that these companies all appear to have been doing all they could when it came to security, at least when we are looking at it from the standard approach of handling security – that defense model of security. I think to some extent they just became the victims of a new approach and were caught unaware. The question to ponder is, how many others out there are running the same standard security model?

[Slide Pg 8]

If we take JP Morgan for instance; I don't think anyone in this room would say that JP Morgan is lax with security as an organisation. But the hackers were after data and the approach of getting through the perimeter and sitting within the networks for a period of time, scraping what they needed to scrape was proven.

[Slide Pg 9]

Sony, a similar scenario. Going back to my statement about Richard Clarke – we need to presume that we will be compromised and the question becomes, when they get in, what is going to happen?

[Slide Pg 10 & 11]

I think when we talk broadly about a hack we need to have an understanding about the diference between a network scenario versus protecting the data itself. All data is not created equal and understanding what needs to be protected inside is critical.

[Slide Pg 12]

As some of you might be buried in your lunch, I will read these statistics to you, however I implore that you do not choke on your food. The Ponemon Instituion 2014 study found that the average data breach costs US companies an average of $195 per record lost, amounting to an average of

$5.85 million per breach. What is more incredible is that Gartner estimates global losses from Cyber Crime to total nearly $400 billion annually.

[Slide Pg 13]

So who wants their logo up here next?

If the reputation damage or disruption to business isn't enough to change tacts before you are hacked, then the financial cost might sway you. We have to start protecting the data itself

[Slide Pg 14]

And why a data centric approach? I feel like we are all on the same page that the current model is broken and that the names I showed you before were not, in every case, intentionally exposing themselves to hackers, they just became victims of the inevitable - absent a new hybrid approach of course.

We know that cyber criminals are out there and that hacks will occur, so let's stop focusing on the hacks, let's focus on the booty that they are after – the data. By securing the data itself through encryption, it becomes worthless to the hacker, and there are policy and protocols attached to the data that deters a cyber criminal from sitting in your systems for months, sucking up what's inside.

[Slide Pg 15]

I've introduced the buzz words encryption and policy – neither of them that novel – but I ask you, what's the point of encrypting something, if you can't verify who you are giving the key to, or without articulating why they should have it?

[Slide Pg 16]

The three critical components of data centric security are Key management, Identity and Policy. Again these are not novel but for us to collectively move forward towards a proper way to securing data we need to understand these three elements of data centric security. Businesses have, clumsily, stitched these three components together however as we discovered earlier, when you stitch security products together, you are invariably left with holes. These business processes must be baked in together at the core of any business security architecture to ensure a holistic approach to data centric security, and here is why.

Firstly, let's look at key management. Encryption is encryption is encryption. There should not be anything novel or revolutionary about encryption because if there is you will not have the credibility or assurance that the crypto libraries and processes have been rigorously tested or approved by the national bodies that approve cryptography. There are ways to strengthen the implementation of your key management, for instance at Covata we employ best practice of one key per file but before generating and issuing the key to encrypt, an identity and authorization challenge happens first.

So we have encrypted our blob of information and tied it to an originating identity - which could be a person or machine. Now we know that it's coming from a trusted source and we have non-repudiation of who created or originated the file blob. This is critical to engender trust of blobs over the Internet in a data-centric security landscape.

However as I said earlier, what is the point in encrypting something if you don't know who you are giving the key to. This is where recipient identity must be tied into the puzzle. It is paramount that you ensure the person or device that you are sending the encrypted blob to has the correct permission to access the data - identity and policy.

As we know, the Internet was designed to share information, however just because you are sharing something with someone or something, doesn't mean that they should have access to it. I think there is a very important distinction there. There is a difference between what I want to do and whether the organisation wants or allows me to share the information.

And finally, if you have tied encryption to identity you invariably come to the conclusion, as we at Covata did, which is to implement policy – or a way to impose control over the data you are protecting. And with the policy side, you ultimately have compliance. For industries such as finance or healthcare with, Sarbanes-Oxley or HIPAA compliance, this is an extremely important piece of the puzzle.

Let's look at a few real life examples from some of customers to better understand this data centric approach.

The history is that we started out in Defense and some of the "intelligence" areas of government. In government they have requirements around the classification of a file and the need to protect it. We have a file sharing solution that using encryption + policy + identity as the underlying security principle allows us to control who touches what as government employees create, send and receive information. If I have created a document and I want to share it with three of you in the audience. I might think that I am allowed to share it with each of you, however in line with the classification protocols within Government, only one of you has top secret clearance and this document is for top secret eyes only. As a result, just because I want to share it with you, does not mean that you should have access to it. Tying that key issuance to the policy means that the identity piece must match up before the information is decrypted.

Another interesting example is research from banking and finance. I am sure that no one in this room has ever received a piece of research that they did not pay for, however it is well known that it does occur. Being able to protect research in the screens so that no one is able to forward it on or download it is an important data control component for protecting IP [Intellectual Property].

Thirdly, and I won't go into this in too much detail today is the whole discussion around IOT and IOE. The way that we are doing things at the moment is not going to scale to where we need it to be to protect the new world that is coming. Again, knowing where the piece of information came from is going to be a really important part of the equation. Let's take for instance the roll out of smart meters, something many Governments are looking at. The whole idea is that they will send messages every day through a gateway in the home or small business to a central point. The data will then be collected and essentially the aggregation of that information will drive power generation for that city or country. The savings in coal generated power are expected to be substantial. All of that information needs to be protected. It might not seem like much when you look at it from the individual homes perspective, but when you aggregate that data, and if you spoof all of those data points as a terrorist organisation, it is a good way to bring down national power grids.

[Slide Pg 17]

A data centric approach, combining Key Management + Identity + policy ensures that whoever touches your company's data, wherever it resides – in the cloud, on a network, or as it is shared – remains not only protected but leaves a clear, identifiable audit trail.

I have given you all a few real life examples of how a data centric approach, typing ID+Policy+Crypto together protects one of our businesses most valuable possessions, its data but the importance of this approach spans far deeper than this. Imagine you are a person entering loan application data, and sending it to the cloud, this is really no different to a sensor on a personal medical device sending health data to the cloud.

[Slide Pg 18]

This reference architecture of a data centric approach really inverts how you think of data security. You can see that the center is key management, identity, and policy - as a unified connected service for the data. It need not be deployed together and is best deployed at least on separate virtual machines and ideally across varied locations and infrastructure. Ultimately the separation of duties principle applies to the distributed approach to data-centric security.

By taking this approach, the data can be anywhere - inside the company firewall, in a cloud, on a vendor's infrastructure or on a mobile device.

[Slide Pg 19]

It's virtually unimaginable that we don't move towards a new security approach for the future of the Internet. Frankly, is plainly obvious that more of the same doesn't cut the mustard - or as a southerner would say "that dog don't hunt."

The agenda of new approaches is not being discussed as it should be. There are too many enterprises and government agencies with too much market credibility to lose, or bury their head in the sand.

I would encourage everyone here to begin a new look dialogue. What I have presented today is not the silver bullet. It will need to be augmented by traditional network security. What it does do is go some way towards leading us to a new paradigm and once we all agree that a new path is required - other innovative solutions will come along to protect all of us.

[Slide Pg 20]

Thank you for listening and I will be here after lunch for those that want to discuss this further.

--- End of Transcript ---

About Covata

Covata enables true ownership and control over your data in the cloud and over mobile services. We deliver data-centric security solutions without compromising simple usability; providing true end-to-end security. Your data is always protected wherever it may travel – inside your network, beyond the domain, to mobile devices and to the cloud – with granular access controls that extend to external ad hoc users, view-only restrictions, real time revocation and complete visibility and auditability.

Own Your Data, control your data and choose where it is stored – with complete assurance that it is protected and secure. For further information please visit Covata.com.

Covata Media and Investor Relations:
Nikki Parker
Vice President Growth and IR
+1 (571) 353-4273
nichola.parker@covata.com