ASX ANNOUNCEMENT | COVATA LIMITED

Sydney, February 3rd – Covata (ASX: CVT) and Cisco Event Speech Transcript

Covata CEO Trent Telford: The Future of the Internet of Everything (IoE) and Security

Good afternoon and thank you all for taking your valuable time to come here today and hear about what both Pankaj and I think is going to be the most exciting aspect of technology, and technology-related investment, the Internet of Everything (IoE) and security.

I'm sure you will all agree that Pankaj's presentation was first class. IoE really is the next frontier of the Internet and every aspect of how we live and do business will be disrupted over the next two decades. I for one am strapped in and ready for what will no doubt be the biggest wave of disruption yet.

I want to use the next 15 minutes or so to take you on a journey into what we are up to for Cisco and more broadly for the security space as a whole. There are some major shifts happening in the security world and we want to explain to you how Covata intends to be the solution.

Let's start up front with what the primary challenge all Internet users, both businesses and consumers alike, are faced with so we can understand why the problems in front of us absolutely need to be addressed.

Few, if any, technologies have taken over our world as completely and quickly as the Internet. It really is a beautiful thing. It is open, easy to connect to, with little overhead, and is relatively simple to use. It has become a great platform for efficient communication, the sharing of business and mission critical information, and collaboration. And I think we would all agree it does a great job of this task! Because that is exactly what it was designed to do. The Internet was never designed to be secure, it was designed to share information. What's more, with ubiquitous connectivity and innovation, just about every activity of daily life now happens online.

Despite its prevalent use, the Internet was never designed to be secure. To provide the element of trust, and allow new applications to flourish, security needed to be added. Many security strategies began with a medieval castle approach: walling off, via firewalls, respective areas connected to the Internet with the hope that adversaries would not breach such walls. To share information between castles, Virtual Private Networks (VPNs) were used to create secure tunnels to transmit data. Again, they are an afterthought, costly to implement, labour-intensive to maintain, and attackers have made a sport of penetrating the gaps and stealing data.

The walled castle approach was okay for a while, for the first five-ten years of the Internet. It's not really adequate now – in fact it's REALLY antiquated. Just ask Target, JP Morgan, Anthem, the White House, the Pentagon, the DoD (CIA/Snowden) and numerous others that have been affected by data breaches.

So what did the tech industry do to try and augment network security for the safe transfer of data – it introduced encryption! Now we can encrypt a file and move it around and it's "safe!" Well sort of. Someone or something has to manage all those encrypted keys. "Manage" you ask – what exactly does manage mean? Well who are you giving a key to? – Should they have it? How do you take it back when they shouldn't need it anymore? With so many questions pertaining to one key or piece of data, the biggest question becomes, how do you manage this daily, let alone over fifty years for regulatory or compliance or audits?

The unfortunate answer is that all too often, we don't.

I won't name and shame you all, but without raising your hands, who here has used an unsanctioned consumer application to send and receive files at work instead of finding a secure, encrypted route to do so? Research from analyst firms all show three to four out of every five employees are using consumer apps for work. The old ways of "encryption" and "security" are put in the "too hard" basket and people, unfortunately, look for ways to work around security.

Even when an enterprise or device company (think Apple iphone) implements strong encryption, it invariably enters the battle between consumer privacy rights vs. governments wanting a 'back-door.' I'll talk more about this shortly, but it is increasingly becoming a challenging minefield with few, if any, players stepping up to help provide a workable solution.

Let's understand the macro shifts that have caused the old ways of protecting data to become inadequate, in so far as day-to-day data security. For brevity, let's focus on the big culprits – smart mobile devices and cloud.

First, mobile devices mean data is no longer locked to your computer at work – it's on your phone, on email, on local corporate or other apps. It walks in and out of the building every

day, sits in your pocket, or flies from one country to another on Qantas. That's what the firewall was designed to stop. We had 'VPN' access remember – so we could 'look into the company applications and data from the outside' – but that's just it – it never left the bosom of the corporate nest – we had to look IN. The proliferation of mobile devices in the workplace changed all that. Your corporate data is now accessible everywhere.

The second culprit was Cloud services. The IT department tried gallantly to lock down the applications and networks in use – but Board and Management asked, "Can't we save a ton and hit this year's bonus pool ten times over if we move core enterprise apps to the cloud?" To keep productivity high and costs low, IT departments have almost been forced to adopt mobile and cloud based applications, ultimately opening up "authorised holes" to allow corporate data to move in and out. It is these holes, as terabytes of data flow through them, that have caused corporate networks and firewalls to buckle and companies to get hacked.

Now for the real zinger. Let's parlay these problems into the emerging tech landscape that Pankaj has now articulated to everyone here; that IoT is going to blow the number of machines connected to the Internet out of the water, and hugely increase the number of transactions we see on the Internet. How's the perimeter and firewall model looking now to you all? It's still looking fairly inadequate I'm sure you'd agree, but now by a factor of X squared. Thankfully Cisco had foresaw the need to solve this little matter - and here we all are today!

As most of you know, more than eight years ago, we at Covata developed a data-centric approach to security, Secure Objects, with the goal of advancing the way transparent cryptography can be implemented, managed, and leveraged. Our patented approach to securing the "data itself" is different and it is this unique technology which will form the foundation for the ground-breaking new product we will unveil today.

But before we do, let's understand Secure Objects a little better.

Secure Objects combines what we believe are the pillars of data security; Identity, Policy and Key Management.

A key is related to one or more authorised identities. Each identity's rights and privileges to a key are captured by access control policies. Covata technology is built on the notion that key management, identity and policy must be a unified, integrated capability and that anything less is a security compromise.

As a quick recap:

1. **Identity** determines who/what can obtain a key and by verifying that this identity has an authorised credential to access the data.

2. **Policy** imposes a second layer of checks that are applied after the Identity credential has been authorised. These checks must be satisfied before the key is issued.

3. **Key management** is achieved by designating a unique key for each piece of data.

Our approach to data security is unparalleled and in demand. How do we know this, because we talk to the global leaders in security. We talk to US and UK government agencies and to our key partner at Cisco in Pankaj. We talk to the biggest financial services firms, industrial companies, healthcare organisations and telco's in Europe and around the world. It's a world theatre and we are extremely privileged to be consulting with the biggest stars and players as part of the script for the movie we are releasing; and its resonating.

And without further ado I would like to unveil to you what we believe will be the future of security on the Internet.

From what I have already told you, I think we all agree that perimeter securities have been trying unsuccessfully to constrain the Internet. We have been trying to beat a wild horse into submission. To make it do something that it was not designed to do. Today we are launching **Covata Key-as-a-Service** (KaaS). A modern approach to security that enables everyone who enjoys the creativity and openness of the Internet to continue to do business securely with the same ease and flexibility they expect. Key-as-a-Service will be made available later this year to the open developer community after its initial deployment with Cisco.

Covata's Key as a Service provides a framework for protecting content wherever it resides, it supports policy driven access, and allows for full access remediation. KaaS combines the elements of Security, Privacy, and Accessibility to build confidence that all data can be moved and shared without losing control of it.

The proliferation of privacy regulations, connected devices, connected software, cloud resident data, and individuals needing secure data access anywhere, means many organisations do not want or have the resources to manage keys, or process associated governance and compliance requirements. That's where we step in!

Organisations need a lightweight way to secure data that can grow and evolve with their business needs. Covata's global Key-as-a-Service will be the standard security protocol that will maintain the integrity of the open Internet.

But why is Covata's next generation of security important going forward?

Trust and governance around encryption needs a reset. It will happen, with governments having a hand in it to varying degrees. Enterprises need to plan for future requirements and be prepared to rapidly address new data security policies and not be caught unprepared.

Covata's KaaS will allow organisations to eliminate the burden of key and access policy management. It is able to adjust according to data security requirements, as business needs change. KaaS will help guard against upcoming legal and regulatory issues, through techniques such as key fragmentation.

Now let's look under the hood - What is inside and how will it work in the real world?

There are a lot of key new features that make KaaS a compelling product - however I will focus on only two of these today.

Firstly, our patent pending Geo-Location process which allows Data Sovereignty to be achieved. The Covata KaaS helps organisations address increasingly stringent requirements for data sovereignty in a manageable way, by shifting the focus from trying to control where data is, to controlling where the keys that protect the data reside. KaaS eliminates the complex, hitherto unresolved issue of protecting billions of pieces of unstructured data. Access to a key is only granted after validating the location of the corresponding data. If access is requested within the data sovereign jurisdiction, then the policy permits the release of the key.

As a real world example, one which will surely resonate with those of you who travel often for work - you have just travelled to China and don't realise that your phone or data has been compromised. Unknown to you, a request to open encrypted data has been sent to the US key server. Thankfully for your business, Covata's geo-policy technology blocks any key from being issued to data that is not physically within US borders. Data sovereignty is achieved through Key Sovereignty – a genuine security revolution and one we think will solve this major twenty-first century hurdle.

From an enterprise perspective, a Swiss global investment bank could sign up to the service and choose for example, Swiss, Singapore, US and Australian key services. Now, the data from all those regions can be locally controlled – similar to the first example, US data cannot be opened in Switzerland and vice versa. In addition to corporate governance compliance, think about how this will legitimately help solve the compounding issues we are facing, especially with the collapse of the European 'Safe Harbour' laws for data transferred between the US and Europe.

The second major patent pending feature is Key Fragmentation, which is designed to help governments appease consumer privacy advocates and help CISO's achieve the balance between government access and customer privacy.

Key Fragmentation creates a special key for a new Secure Object. This key is *fragmented* and then delivered to four different data custodians. The first fragment is kept within the Covata KaaS. The second fragment is sent to the government, or duly authorised agent of the government of the sovereign state where the generating key service resides. The third fragment is sent to the tenancy owner or its nominated escrow agent. The fourth fragment is sent to the auditing firm of the Covata KaaS. Federal, or authorised agency parties can access a whole Secure Object's key by obtaining a duly presented court or similar order from the legal jurisdiction of the home key service.

So, when the Swiss Investment Bank from my last example, signs up and selects 'key fragmentation' on one or more of their servers, a copy of the key that encrypts the data file is then broken into four pieces. One piece will be held by the KaaS, the second by the bank, the third by the US government and the fourth by the independent KaaS nominated audit firm. Let's say for example in three years' time a US supreme court order is presented to the Covata KaaS, the four parties can hand over their key fragment without any grey areas of "Why should we?" The government gets access to the data without consumer or corporate stoush and the bank gets to have an arms length association with this very potentially messy compliance piece. Consumer advocate groups are generally happy as the government only gets access to the data through a rigorous and open process - not just snooping.

It is hard to imagine how important this issue is becoming. China has just passed a new 'anti-terrorism' legislation that forces telcos or other Internet companies to provide a decryption service in the event that the government suspects terrorist activities or that extremist content is being distributed; China is quoted as saying "it's no different to what other countries in the world do." They may be pointing at the US or the UK, the latter of which is grappling with introducing the so-called 'Investigatory Powers Bill' which alongside extensive monitoring places new legal obligations on companies to assist these operations to bypass encryption (open it up). The 2015 Global Encryption and Key Management report from Thales e-Security and the Ponemon Institute backs this up. Interviewing over 4700 business and IT managers, the report is now in its tenth year. Key Management is identified by over half the respondents as a major issue.

The Covata KaaS with key fragmentation process is intended to be operationalised with the appropriate legal and jurisdictional aspects for each country Covata operates KaaS in. In other words, horses for courses in each country and we are taking this burden off everyone from a software developer of apps to the largest Fortune 500 companies. The Key Management burden is handed off to the KaaS and paid for up front for the life of that key or service requiring the key.

This revolutionary key fragmentation service, along with the reassembly process and the routing of key requests to the right country for the given data, is also a patent-pending aspect of the new Covata solution.

What makes the Covata KaaS so ground-breaking is that this secure process can be done at global scale. With KaaS, data can be shared securely from person to person, machine to machine, corporation to corporation, in the cloud or over mobile networks; wherever it needs to travel. And most importantly all of this “hard” security will be done without the application or service owner having to “do” security or encryption or key management – they just get on with what they are doing today and use the KaaS to do the encryption and access control.

As we move into the world of IoE that Pankaj described for us, this intrinsic security process becomes vital.

Just imagine, a large company has machines and equipment out in strategic sites for mining or agriculture or monitoring. Each little blob of data created, held or sent from these IoT devices needs to be secure. Why? One piece of data, or a few pieces of data, are unlikely to be of much value, but keep in mind that the data from the field is being sent to a central location, usually a cloud or big data service, where it is aggregated and used for decision making. Much of this data will be moderately or extremely sensitive. A hacker could be watching all that data traveling “in the clear” up to the aggregation point. That hacker could find out what’s going on before the company - and the ramifications of this knowledge in the wrong hands speak for themselves.

The fallout from this example could range from terrorist attacks shutting down vital operations such as power or transportation systems to stealing market sensitive data on everything from agriculture yields to mining outputs. It could be stealing the design blueprints of the latest electric car being sent to robots on an assembly line. The issue of security in industrial IoT are wide spread, and very real.

This is why the Covata KaaS will simply do this work in a standardised way for companies and IoE innovators. We will protect each piece of data and importantly, the data never passes through the key server (or any part of Covata) – end-to-end encryption is the hallmark of Covata. It goes from device to wherever it needs to be sent! We just allow it to be encrypted first and ensure only the authorised intended recipient decrypts it. Let’s not forget that in this whole process, full auditability and compliance is achieved.

The users of the service, once it is made available to the open market, will subscribe to the Covata cloud-based Key Service and the users will pay for the keys. Keys could range anywhere from a fraction of a cent to dollars - it will all depend on volume and the level of compliance the customer seeks. With KaaS the security of IoT can be built into the operating costs of the business model from the outset with life of device support.

We are extremely excited by this new paradigm shift in data or object-based security. Importantly, for any big vision or new standard to emerge as a real player, momentum and

take-up is critical. We are keenly aware of this and thus our timing of launch over the course of this year, and to whom it is launched, has been honed upfront.

Pankaj and his team at Cisco were excited by this early on and are of course the first to come on board. Later this year after Cisco, our government, telco and corporate customers will be able to upgrade to the new 4.0 version of Safe Share with geo-location – allowing data to be locked, tracked and managed anywhere in the world according to the device it's on and where the device or person is located. This truly is a corporate data governance revolution for mobile. Think of what this means for Foreign Affairs Bureaus, Defence Departments and multi-national corporations – let alone the IoE landscape.

The world is only going to become more and more connected. More and more data is going to be created and collected. While the rest of the security industry is still trying to work out a way to secure the unimaginable influx of data – Covata is unveiling its patent-pending Key-as-a-Service solution today!

Thank you everyone for joining Pankaj and I today, and being the first to hear what we believe will be the future of IoE and Security.

Media and Investor Relations:

Nikki Parker

Vice President Growth and IR

Covata

+1 (571) 353-4273

nichola.parker@covata.com

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 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.