# Title: Securing the Digital City: Cyber threats and Responses

Subject: Safe Cities

* Safe Cities

Abstract:

As cities embrace digital infrastructures to improve the overall quality of life, new potential cyberattacks due to numerous vulnerabilities may arise. This influences how cities design, implement and maintain their cyberdefences. Distributed ledger technologies offer considerable promise. How can public safety organizations learn to leverage these technologies appropriately? What role can self-assessment tools play in securing the digital city?

Speakers:

#### Joe Paiva

#### Alison Brooks

#### Munish Khetrapal

#### Ian Smith

#### Asaf Ashkenazi

Conference:

hey while everyone's still focusing

while people are still coming in I just

want to say that there is an asking vote

application and once everyone's in I'm

going to explain how to use it but we

really do hope there are a lot of

questions because smart cities is such a

big topic and cybersecurity is such

a big topic and distributed ledger

technology is such a big topic there's

so many topics out here really hope you

ask a lot of questions both in person

and via the app so I think the room is

full now so I'm gonna go ahead and get

started because we're already kind of

the clock is where I took us down to

about 50 minutes here so let me first

thank everyone in the room for coming

this is a big crowd the room is full and

that's that's a good thing there's

nothing worse than coming up on stage

and having like three people in the

crowd which makes it nice and intimate

but very awkward so we have we have just

about every seat this is this is like a

Catholic Church where I grew up every

pew is full except like the front row

the but but so let me let me quickly in

in in addition to thanking you all for

coming out like the people that jumped

up and got the front seats there's an

asking vote app on your own for those of

you who have downloaded hopefully the

smart cities app for the event app we

want to make sure we get to your

questions we really want this we have

set up this panel so instead of doing

presentations up front we're gonna ask

ourselves if I'm gonna ask them a few

questions they're gonna tell a little

bit about themselves and answer those

questions and then hopefully we'll get

lots of questions from you so the more

questions we get the better if you

haven't tried it yet could you please

take out your smart phones go to the app

and when you're in the app you click on

the ask and vote option and you can

select this panel and and when you do

that it will let you ask questions

because I know a lot of people don't

like to run and you know fight to get to

the mic so please do that please open

your app go to the it's called asking

vote it's towards the bottom and then we

click on and it gives you like

menu with menu buttons four three four

three rooms

please select ours and then and then

you'll be able to start asking questions

in real time so with that and if you

don't like the app please grab the mic

when the time comes so my name is Joe

Paiva

I am the CIO of the US Department of

Commerce international trade as US as in

the United States and you know kind of

here's the thing from traffic jams in LA

to traffic tickets disappearing in

Melbourne two major meltdowns in Germany

we've kind of all heard about the

threats related to the Internet of

Things and and by extension to smart

cities and we've put together panel

today that I think comes from a pretty

varied background that's prepared to

talk both at a high level and if you

guys want we'll go as deep as you want

into ways to address these these cyber

security challenges so with that I am

gonna start out with the end and I'll

let each of these individuals introduce

themselves tell where they're from and

kind of give their their three minute

spiel view from the tie level and then

we'll dig down into some my questions

and then hopefully into a bunch of yours

ok thank you that's just check same

check on the mic okay and so it's great

to be here I'm Ian Smith from the GSMA

and I'm the IOT security director Jason

May I think probably many of you know we

run a small event in Barcelona called

Mobile World Congress every year now

what do we do with the the money that

that conference generates well we're

not-for-profit trade association all the

money that's generated by GSMA goes back

into solving industry problems making

the world a better place and one area

that we've been focused on in the last

24 months is a whole issue of cyber

security in particular relates to cyber

security of the Internet of Things and

the smart city kind of personifies the

challenge the Internet of Things brings

you know look all the diverse use

in the small city you see them back

there in the Hall hundreds of different

use cases from you know metering traffic

pollution and so on on the surface of it

this looks like a really big

cybersecurity challenge it needs to be

solved and I guess I guess it is when

you look at it for a use case

perspectives very diverse looks like a

big problem but when you boil this

problem down actually when you look at

the platform's the technology that sits

behind it there's actually a lot of

simplifications that can be bought and

when you look at it from an attackers

perspective there are only really a

fewer methods of attack that can be

applied to smart cities so if you to

apply these simplifications it's quite

easy to generate resources such as

security guidelines security assessment

schemes that can help you you know

ascertain but firstly define what

security you need and secondly measure

the security that's being supplied to

you by your suppliers by the solutions

that you're looking at and that's what

we've done at the GSMA we've develop

security guidelines which are freely

available to be used we've developed an

assessment scheme which you can use to

check measure the solutions that are

being offered to you both of these are

freely available resources on our public

internet for you to download and use so

that's what I've been doing but today I

want to have C hear your questions and

hopefully give you guys some insight of

how our guidelines how our resources can

help help you solve some of the problems

that you've got in deploying this

technology ok so thank you munitia

thank you welcome good afternoon I hope

all of you are not gonna be sleeping in

this session there's a lot of threats

out there so there are about 20 billion

sensors and smart cities that are going

to be connected it's gonna create about

three trillion dollars of incremental

value 20 billion sensors three trillion

dollars it's there two messages you want

to take out of this session but after

these twenty billion sensors or as these

twenty billion sensors are being

connected over the next five to seven

years you're looking at a lot of IOT

threats and if you go back from 2000s

that there are so many threats one of my

favorite things as a 14 year old kid who

used remote control in Poland and

thought about the tram station as a

Stice station

and he actually changed the tram timings

using a TV type of a remote control and

that he did about four or five years

back and then their blackouts in Ukraine

there lots of different cyber threats we

are seeing over the last one year alone

there's an 310 percent increase in

threats because of IOT devices 90% of

them are becoming from IOT devices three

primary reasons and this is

oversimplification there are many many

more reasons but at a high level the

first reason that we are seeing the IOT

device is creating a threat it's just

the knowledge base for the IOT sensor

companies because there's a lot of

innovation happening in this market a

lot of it driven because of smart cities

these sensor companies come from

material science background they're

they're looking at ultrasound they're

scientists while thinking rethinking how

to digitize physical space they don't

have knowledge in context of security so

they don't implement anything in

security and that starts the first set

of threats that get created because of

that the second is just insufficient

resources they take an existing parking

meter and we say that parking meter is

going to be connected you have a $20

chip you go and connect it and you send

it back to the network and now since

it's connected you can have a mobile

phone and you can make payments great

sounds good makes money but if somebody

hacks into the parking meter and goes

into the parking application he can

download all consumer data and we know

there's some threats like in the u.s.

systems like HVAC systems were used to

download all the customer database of

target retailer those of you from us

will know that so it creates a lot of

things

the third is market pressure we're

seeing a lot of pressure and I was

talking to a lighting company and we

partner with a lot of these sensor

companies they help to complement our

solution and this lighting company says

hey I've removed the security module

because the public sector tendering

process is so cost Previn and sensitive

that it doesn't make sense it they don't

ask for it so why do I paid for it

so you see different reasons why RT

devices create these threats now of

course our strategy is to create an

overall IOT threat defense framework

we as a company are focused on creating

the network so we consolidate all sensor

data and application data that can come

from endpoints we securely connect those

sensors and devices and then transfer

transit translate them through the

network into into applications that can

consume it again all through API is an

encryption and all types of different

technologies and tools we use but our

goal really is to start step working

with the with the cities and thinking

about our ecosystem partners working

with standards bodies to bring in a

holistic strategic framework on how to

address cybersecurity there is three

trillion dollars of value to be

generated in cities by connecting

sensors and devices so one approaches we

don't connect and we don't create that

value second as we create a holistic

framework and work with ecosystem

partners and sensor companies and look

at different standards that we can

enable and certify them and deliver

solutions that provide value to the

cities so I saw too many places at once

so my name is esophageal Ozzie and I'm

working for rhombic rhombic is a

us-based company and we are doing

security product probably most of you

are not aware of us but you're using our

technology almost any smartphone that is

a manufacturer that means probably in

your pocket is having our security

technology and I think that most of the

credit card on this small chip that you

have there has a security products and

we're working also security products for

for IOT so you know one example that

I'll get that it's not like the examples

of the attacks that people are talking

about it's actually different example

since I live in San Diego ethnic close

to LA we had in we had a Hollywood

producers coming to us and they wanted

to do a movie about cyber attacks and

they wanted to make it more realistic so

they said let's ask about the real stuff

off of what's going on and how the

attacks are being done and you know they

were left they

them that the meeting they were not

happy because they thought that it will

be like you know in the movies and

somebody is hacking and when we

explained how actually simple it is and

what are the attacks are there they were

saying really and of course they don't

they didn't use any of our stops in the

movies the movies looks much because

nobody will go to the movie but that's

the thing the thing is it made me think

a lot of the attacks are simple and

straightforward I mean it's it's

sophisticated in the way that they how

they thought about it but at the end of

the day it's not that complicated and

you think about it you're saying how

come we left it open why there was no

security there and when you look at the

IOT it's even more saying there are

security methods that are being used for

the past 20 years that we are using

let's say in browser and others and then

still 70 percent of IOT devices have no

authentication and encryption and you

start to look into that and you find out

that the main reason for that is that

security is too complicated for reality

because IOT is simple it's actually more

difficult to do security it's more

difficult because the devices don't have

a lot of resources it's more difficult

because some of the companies that used

to do things that are not connected they

don't know about security and it's more

difficult because the scalability of

these things if one device is hacked

it's not the big problem in IOT but if

now you have a lot of devices and they

are whole can the indeed the attack can

be duplicated then it's a real problem

and I think that in order to to get

security adopted more in IOT and smart

cities it needs to be more

straightforward and work so the people

you guys that are building the wonderful

ideas that will make things more

efficient and will help everybody will

not have to think a lot of security

because it will work and it will be

solved if you need to spend your time or

resources over and over to recreate

security then we have a problem so I

hope that security for IOT

become simpler and more affordable for

everybody and Allison hi everybody my

name is Allison Brooks I work for IDC

which stands for the International Data

Corporation I'm on our global smart

cities team and I'm the public safety

specialist and when I think about the

whole area of securing the digital city

I'm really sort of faced with the

reality of what cities are struggling

with and for me that's the struggle

between all of the old old legacy type

technologies that we see you know you're

just a classic end-user devices printers

which if you look at any of the

procurement RFPs out there very few of

them actually have security

specifications written into them to any

kind of level of sophistication that

we're looking at now but then I also

think that cities are struggling with

those legacy technologies but at the

same time new and emerging technologies

like distributed ledger technologies

like bakhtin and those are creating

additional complexities for law

enforcement and public safety and that

it requires a completely different way

of conducting investigations or going

about your day-to-day business

so I'm sure you're all familiar with the

Silk Road example of the sort of darknet

marketplace from a number of years ago

basically when that whole thing went

down the law enforcement study eight the

Department Homeland Security

investigators really had no idea when

they first started getting into it about

what what and how they were going to

investigate and prosecute they weren't

sure if they were going to target

blockchain itself

Bitcoin the websites the people they

didn't so they had to start from Ground

Zero and figure out you know teach

themselves basically digital blockchain

technology and how to actually go about

prosecuting in that dark dark net

marketplace so I think that when you're

looking at smart cities themselves they

really are struggling with that old the

old technology and the new technology at

the very same time and it's a completely

sort of new you know black mirror kind

of world that everybody's dealing with

fantastic so I guess the first question

I'll ask all everyone up here is this

we're going no special order to answer

but maybe

start with you and so is this all too

much like is the juice worth the squeeze

like so so every once told us how how

bad things are what's the positive sign

right like what is what is the benefit

of doing this okay in terms of the

positive the only thing we can see that

in the whole there I mean all these use

cases bring great benefits to to cities

in terms of you know proving air quality

proving the efficiency of city improving

the quality of the transport systems and

so forth so you know the net effect

should be great on the citizens of the

city I think we will buy into the use

cases and the benefits but this security

piece I think is is is a real you know

an inhibitor to this these these use

cases becoming real and then everybody's

lives in a daily basis but I think the

positive sort of green chute that sort

of sits there is that these challenges

are challenges that we've overcome in

the past okay

many industries have overcome these

these challenges and the IOT can

leverage a lot of existing resources

technologies capabilities that are

already been developed and the good news

is somebody else has paid for this

technology already guys you know the

fence industry is probably paid for a

lot of it the telecoms industry is paid

for a hell of a lot of Technology you

guys can come and use it but you need to

know what to ask for

and you need to check what your

suppliers are giving to you and that's

the real challenge I've heard it time

and time again for the other panelists

here people aren't asking for it

people aren't bending it into their RFPs

that needs to change but I think if you

do you'll find good answers you'll ki

find your vendors and your solutions

Freud is giving the right arts its back

but they're all gonna do that unless you

put it in the RFP because that's gonna

push up unfortunately the cost of the

solution and I think fundamentally we

come back to that cost word and that's

probably the big challenge don't we we

all need to overcome but I think they

will probably come back to that

discussion several times in this panel

and I won't start it just yet

so ask if you want to take a stab at

that one too sure when I look at

technologies you know when we were not

me I'm not that also when we people were

riding horses and carriages right and

and you know and the automobile came

everybody said oh this is a terrible

technology people will die because it's

like so dangerous right

and then you know over and over when the

internet came they're saying or now it

will be a cyber disaster back to that 2k

back you remember that

2000 in the world will come to an end

and now I see it again it's the IOT it

the Armageddon of IOT that the machine

will take over us so I don't think that

this will happen right so I think that

sure there are risks but the benefits of

IOT of making things efficient

especially when you're talking about

smart cities and the benefits for each

one of the citizens of this city's is so

big is just that we need me to make sure

that we also take security and make sure

that it's protected but I definitely

think that the benefits is much much

higher than the risk so somebody call

audible here because because before I

before I throw it to Cisco so the fact

is that that automobiles do kill

millions of people right that horses and

buggies never did and and and the fact

is that I would argue the the the stakes

are much higher we've left the $2 in a

blackjack table and we're now at the

million dollar blackjack table right so

so I'll ask you the same question but

but with that as a background right

because I would argue the stakes are

much much higher yeah I remember I mean

I'm not that old but when they actually

first introduced them I don't know how

many of you know this they had there was

a policy that said there has to be a

horse in front of an automobile that's

how they actually introduced it so I

mean yes security is thought about it so

we thought about I'm not sure you need a

horse in front of an automobile to

insure their new accidents but I think

you should take a step back and see

what's happening in the dynamics of the

world by 2050 we're gonna have about two

and a half billion people more in this

planet and most of these people are

gonna live in cities so you're gonna

have each of your cities between 50 to

100 percent more populated in the next

30 years so just think about what

happens to real estate rentals parking

energy consumption water waste so one

way is to have a horse in front of the

automobile that's that's a good way so

do nothing basically or second way is to

say we have to digitize but we have to

come up with frameworks and and

capabilities which the industry has it's

not that the industry does not has not

thought about it and of course this this

is gonna be an industry that's going to

evolve and you're all going to learn

things of that kind and you can start in

in phases and start building secure

frameworks to deal with this opportunity

so the opportunity is much bigger I

don't think it's a question of even

three to three trillion dollars of value

it's a question of if you don't do

anything can you even survive there's

70% increase in population so if you

can't then what's the lesser of the two

evils that's another way to think about

it in a simpler simpler manner Wow you

can be a real downer I think I think

yeah I think we need to meant that to be

an upbeat comment right there's a big

opportunity there but from my

perspective um you know when I think

about the payoffs I look at cities like

New York City we're in the New York City

booth right now with them and New York

City has really been at the forefront of

a lot of these newer technological

advances in terms of leveraging advanced

IOT solutions and video analytics etc in

its real-time crime Center is a Center

in in New York City and using the domain

awareness system that I believe is

Microsoft what it has been able to do

with all of its interconnected

technology is basically stop the stop

the perpetrator by by following them one

block to another aren't on video

surveillance and also then sort of

decrease the time between the response

phase in the investigative phase now now

they say that they're the best

investigations actually start in

response and that's because the quality

of the situational awareness is so much

better that they're able to get to the

seam and finding the actual evidence

before it as in fact sort of removed or

lost or whatever so they're really able

to leverage a lot of that securely now

they have struggled with a lot

the you know privacy constraints around

you know stop and frisk and stuff like

that they still are stopping and

frisking they're just not you know

collecting the database anymore to do

that so there's a bit of a course

correction that they're engaged in on an

ongoing basis and they work with their

privacy commissioners etc but they do so

in a way that's measured and metered and

great success for the citizens of New

York and visitors and tourists you know

crime has gone down there year over year

for the past ten years now I think since

they've been really introducing these

systems securely so they're a great

example of the types of gains that can

be made in the smart cities space with

regards to public safety fantastic

before I ask the next set of questions

could could would you with the audience

mind because this is supposed to be an

interactive session and I don't want to

eat up all the time with the questions

from up here if there are going to be

questions from out there and I have no

way to know so just by show of hands

who's either put in a question on the

vote and ASCAP or plans to within the

next five minutes or is gonna get up and

go to the mic when we open it up to

questions so yeah maybe four or five out

of like a hundred and fifty people so

not not a highly inquisitive group or at

least not an aggressive one but so

please please put in those questions and

and please print as many as you can and

I'm gonna kind of try to ask I'm going

to combine the last two questions to

kind of wrap it up a little bit so that

we can get to your questions quicker and

then I'll save any extra questions I

have for after one last question for the

cloudcrowd before I ask the last

question by show of hands who wants me

to ask a distributed ledger technology

question versus a question about

anything else how many people are really

dying to hear about distributed ledger

technology oh so there aren't there are

there are some people in the room not I

still a minority but I think I think I

could ask anything and who wants a

million dollars by show of hand

yeah yeah at least got ten all right so

so all right so let me kind of let me

let me kind of combine a few things into

one question and and Andy and I'm gonna

it's gonna be a tough cuz you don't know

it's coming right but but we'll stick it

so look we're in a world right now where

we have the average organization has

hundreds of computers big organizations

like mine have tens of thousands and we

have not been able to secure traditional

computers and that's in a world where I

literally patch an update all those

computers every week and I can access

them just by walking up to someone's

desk right or my servers you know go

into the cloud so you know what are we

gonna change in terms of approach in a

world where now a typical CIO for a city

a little city right

who has far less resources than I do is

now stuck with tens of thousands of

devices some of which are buried you

know under a mile of concrete or in very

difficult to get through places right

it's it's a lot easier to patch a

desktop than it is an IOT device in a

sewer system right so what are we gonna

change how are we gonna implement this

holistic approach in this world of IOT

and get better results then then then

let's say we were for the for most of

the past ten years in our traditional

networks okay well well thank you for

the for the basic question that's it's

appreciated

I think you know there's a change of

mindset I mean you talk about the

enterprise today you know the the

traditional enterprise culture where you

have you know lots of lots of computers

connected to networks I mean the

methodology they they adopt their

username password that methodology this

doesn't apply to IOT it's being used in

IOT services today we've seen the

consequences but all these video cameras

being hacked they just apply the same

methodology what we preached with JMA is

to take other methodologies and

particularly take methodologies that the

mobile industry developed we base our

security around SIM cards you ICC's

these are small secure certified pieces

of hardware that are embedded within

every one of your mobile phones and we

use that as our root of trust in your

mobile phone and that technology was

developed it back in 1989 it's been

upgraded since you'll be probably glad

to hear but but the methodology stayed

the same - it said the same

framework stayed the same you'll be glad

to know in each of your sim card there's

an desert there's an updated security

algorithm sitting there dormant that we

can switch on if tomorrow there's a hack

of your of your mobile encryption

technology network operators can switch

to the next generation of algorithm

over-the-air and this is the kind of

mythology that you have to apply to IOT

you have to take similar methodologies

from other industries I say partner with

other industries take technology they've

developed they've paid for and embed it

into your into your devices into your

solutions you can take the OTA

technology that's been developed the

secure hardware that's been developed

the secure application environments that

have been developed reuse them that all

you know updatable over-the-air they all

potentially have a lifetime of tens if

not multiples of tens of years and

really that's nothing the solution in my

views to get to move this forward is to

not go down the traditional enterprise

IT security route but to took a look at

other industries not just the telecoms

industry by the way look at set-top

boxes other industries they've taken a

similar approach to QA Hardware

embedding roots of trust in into devices

and it's all gate can be done at low

cost but it needs to be thought about it

needs to be bought into your overall

strategy for those technologies to be

successfully deployed and that's what I

advocate so so then let me modify the

question a little before I throw it to

you Manish the the if I look at the rest

of the world right so I run today you

know a 500 million dollar organization

but I previous Java had a four billion

dollar IT budget and I found it was

impossible even with a four billion

dollar IT budget to run a world-class

cybersecurity organization and so we

moved everything to the cloud right and

we relied on service providers to do all

that stuff so is is there a play here

for X as a service as the quick way to

roll out secure applications or just

like we do in other industries or where

do you see that going you should have

come to Cisco and you're spending that

kind of money we could have helped you

there

but you know I think so the way we have

approached it is not all sensors aren't

going to be secure that's just the way

it is and we'd love to have every chip

embedded with security in fact we are

working with standards and we call it an

IOT ready Network standard where you

have 256 bit encryption there's

something called a mod file no pun

intended

it's basically manufacturer usage

description file that tells this network

that what's the sensor supposed to do a

parking sensor and similar example we

talked about basically it says the

parking sensor tells you whether the car

is path not parked where is it parked

and for how long it's parked that's all

it needs to tell it doesn't need to go

to the payment application it doesn't

need to go to the IT system it doesn't

need to send reach the reporting system

because that's where the loopholes start

so if you have a way to automate sensors

to come into the network and you can use

the network as a means to segment that

problem you have visibility of anything

that flows in the network then you can

control the security and issues around

in the network stage and that's really

how we have evolved our strategy we've

actually consolidated and we have done

this in industries from the last 25

years whether it's service providers

where we converge wise video data

networks where we looked at enterprises

we looked at Enterprise why is being

converged and IOT now being converged on

to our network and now we sync security

and network converging every device of

ours every switch of us every router of

us has software that you can enable to

sense what the sensor is doing where is

it going

you can set with the radar you can

ensure it goes to the right place

you have visibility you have tools

malware ransomware detection tools that

can even detect patterns even if you

have encrypted data you can actually

detect pattern encryption based on

pattern recognition you can on encrypted

packet so there's a lot of technology

there but I think it's not just the

technology that that's important it's

also the people and the process that you

need to wrap around and you need to

build that whole security framework and

strategy X as a service helps to elevate

many of the comes concerns so we have a

cloud platform

it's called Cisco kinetic for cities

basically it securely connects and

sensor to any application it encrypts

the data stores its segments that it

does a bunch of things we just talked

about and that allows you to the

technology actually allows you to go any

leverage it but even if you use take

blockchain as an example which this is

not breakable but if you give the wallet

to somebody there's nothing you can do

half the peer half the sensor companies

when you install the data sensor actual

sensor and our gateway application you

use standard temp one two three password

three two four five and you don't even

bother to change it so you can have any

amount of security but if you're in our

process to manage that security the

other problem so you have to bring in

the people process people is the

education process and technology

together that can solve these problems

so awesome these questions keep

restating this question to make it a

little more difficult every time so so

so we heard about X as a service over

here but but let me get to the root of

things so nine out of ten of our current

breaches all come down to strong

authentication or I should say the lack

thereof right so I go out in the net

where I go out right now and I bet you

half the people in this room log on

applications with the username and

password somewhere and if you don't know

this any computer you log onto with the

username and password trust me I can

hack in under 20 minutes so so the the

question is where does strong

authentication go as part of this as

part of this challenge for IOT

right so I I will answer that it's a

really good question now I answer it

like upside down right so I'll say

you're talking about passwords that are

bad do you know that what brought down

almost like huge services in the United

States like Netflix another which was a

Mirai

the Mirai attack a botnet that was from

IOT devices most of the attack you know

how it started because they used

username admin password guess what admin

second option first we started really

easy

but this is what brought down right big

sites like

that's the simplicity of some of the

attacks so yes authentication to know

and it's not authentication in terms of

users putting this password it needs to

be automatic so service should be able

to authenticate the device and know that

this is a real device legitimate device

that I can trust and connect to the

network and it needs to be done

seamlessly if I need to have somebody

puts the past or then I have a problem

with that the device it's all should

work really without any human

intervention because we are talking

about millions of devices and you know

the authentication is a good example and

and and of course our product also do

does that but for any product that is

being used what we are trying to do I

think which should be done for IOT is

three things the first one is to protect

the device in terms of make sure that

you reduce the attack surface because we

know that software will have bugs but if

I have strong authentication is strong

connection to the cloud I make sure that

the bad guys that are trying to look for

these software vulnerabilities will not

be able to talk to my device so I

already did something that is very bad

by authenticating and creating an

encryption then the second one is to

have detection I need to know that the

device was compromised so we heard like

different solution like doing analysis

behavior analysis and different others

but this is the second one so first

protection authentic with the

authentication and encryption then

detection because I want to know that it

was compromised and then it's how to

renewal or renewal ability of the device

the devices as I said will be there in

the market for a long time right we

don't know what attacks will come in the

future we have to have a simple way to

authenticate and to resolve the problem

that you will come because the problems

will come so these are the three basic

elements that I believe needs to be done

in IOT to ensure that they are protected

today but not just today also for the

future great so I'm about to pitch to

Allison but can we get the actual

someone's supposed to come up with a

tablet awhile ago that had the questions

on it

and if anyone wants to go up to the mic

because we'll go to Al

listen real quick and then we'll go to

the mic questions but Alison so the last

switch up of the question right and some

people are waiting for this is so if we

want to X as a service and we're talking

about doing authentication right there

has been a lot of you know no one will

tell us how but there's all this

top-secret hush-hush stuff about

distributed ledger technology for

authentication and distributed ledger

technology for better cyber security I

don't want to put you on the spot

because I don't know if you've had a

chance to really kind of I'm throwing

this curve ball at you but do you want

to tell us some places where you've seen

or where you think we will see

distributed ledger technology you know

and I'll caveat that with I don't

necessarily mean blockchain because

that's one of many you know DLT

technologies yeah well I'd go back to

the Silk Road investigations again

because that was a really interesting

application of of blockchain being used

to sort of obfuscate and hide the crime

on you know on one hand but then it was

exactly that that led them back to the

investigators back to the be able to

trace all of the forget forensic crime

being conducted and to bust their own

agents actually ultimately they were

able to go and trace the illegally

siphoned bitcoins that the their own

agents had been actually putting into

their own wallets so the technology that

way has this capability of providing

that you know the breadcrumbs back to

back to to the event and it's immutable

right that's the whole bonus or the

promise of blockchain is that it creates

this traceability at the same time as it

hides things so if you can figure out

the technology and get around it and use

it appropriately you can actually you

know that's that's how they actually

were able to bust Ross Ross Ulbricht

with with with the Silk Road stuff I

think that there's going to be an

interesting play with blockchain and an

IOT in a sort of a more positive light

there'll be like sort of more of your

stadium and events joint offerings with

this say your ticket sales and your IOT

lighting up here you know your way to

your seats and things like that so

there's lots of you know not security

cyber threats sort of you know angles to

this technology as well that are of real

interest and then and of course the e

identity piece of the blockchain in

terms of trying to be able to

you immutably secure your own identity I

think there's lots of problem promise

with that I was talking with an FBI

agent a little while ago about that he's

a little bit scared by the prospect of

ultimately when you know advanced

computing was able to actually sort of

trick the blockchain you know and beat

it we'd be all in trouble in terms of

our identities but but I think that just

means that we have to actually you know

we're not gonna not improve things for

20 years so I think it'll be an ongoing

sort of rolling experience that we have

with the technology and what we're doing

with it but fantastic question where's

that I never do get the thing so I guess

if someone just wants to walk up to the

mic or hopefully someone will where was

this tablet

oh there we go because no one is jumping

up to the mic you know so we're joking

you know there's some parts of world

we're like the mic has aligned 15 feet

long and some parts of the world where

if you don't have the tablet you'll

never get a question so let's say just

wow Oh Swedes up getting a lot of

questions I wish I had had this 15

minutes ago

all right just pick the easy ones all

right so so so all right I'm just gonna

ask each I'm gonna throw this question

you can you share good examples of IOT

solutions using security by design who

wants that one I do not who wants it do

you want it

all right subscribe to keep the

questions let's try keep your sisters

fast you got one minute there are lots

of solutions that have a lot of security

and encryption that we are looking at so

some basic things now we have seen

networks that we're deploying so

specifically for lighting and parking

type of solutions but actually like we

talked about waste management that's

that's the latest one you can go up to

our exhibition booth and you'll see that

this is deployed in the city of Spain

Granada where they deploy waste bin

sensors and these devices are using

Laura technology which again has fairly

good encryption and

and authentication so once you get into

the network we can actually consume that

information and data and provided to the

right fleet so that you can go and pick

up waste city say between 15 to 65

percent it depends on how how much of

waste and what the costs of waste are

this is a huge amount of efficiency and

I think that's a success thing because

the way the network was built and we

worked with the company called Ferrovial

there and and what they they really

thought through the whole security

aspect right through the design phase on

how's the cents are going to be

installed how they going to authenticate

it

how let get activated what would be the

network how the information be sent to

the fleet management applications how

we'll have dual authentication for

applications so that we ensure that the

the people who are using the information

are making the right decisions so

thinking through that right through the

design having the people process along

with it and enabled by ecosystem of

partners that brought us together to

deliver that is a clear outcome that

cities are consuming and I think that's

a replicable solution same thing for

parking and lighting so here's one I'm

gonna give this one I think to you

Allison the the question was do you

think we should start applying penalties

to companies IOT companies that

introduce the cyber cyber I guess shall

we say gross negligence in terms of

cybersecurity and IOT systems do you

think we should start applying penalties

to them that's the question on the table

making them pay for their sins I mean I

think there's already so you know I see

a system of fines if you know things are

egregiously handled but I'm not sure if

that would I don't know that I actually

would be a deterrent in fact to it

because I think that it's gonna happen

regardless of whether you do that I

think it's they that they operate it

with under factors outside of that kind

of deterrence I think it's fair so

there's one in here about hl7 which you

know being a healthcare CIO in the past

I'm a little bit biased on this if I'm

going to ask the question anyway so if

one of you guys want to take it is it

feasible to have all IOT devices use

unified communication protocol and and

they say like biomedical and health

information systems which for those of

you don't know are the most insecure

systems in the world they make smart

cities look good but but but who wants

to anyone want to take that there you

know I think I think the answer is no I

mean I've teach this to diverse I mean

you've got lots of lots of use cases

lots lots of different business models

they were all going to require solutions

that meet the cost targets that

pertinent that particular use case or

the particular use cases it's a whole

variety of different communication

technologies are going to be used you

know from you know speaking myself

you're going to have LTE devices 4G 5g

devices narrowband IOT devices LTM

devices 2g devices Bluetooth devices you

know every technology spectrum is going

to be used I don't think that's going to

necessarily converge anytime soon

because you've got different solutions

trying to hit different use cases

different cost targets but the good news

is is that for every one of those

technologies there is a tech there is a

solution to resolve the security related

to those the communication path the

problem again is those technologies need

to be applied needs to be played on top

of the communication technology itself

and needs to be implemented it needs to

be integrated and that's probably where

the challenge comes that's where the

cost comes from ultimately the customers

going to pay that cost to get the secure

service very well so there's one

question here that I'll just answer real

fast it says are there procedures in

place to standardize the deployment of

security measures and how could these

procedures cope with state-run attacks

I will shamelessly plug that the

National Institutes of Standards and

Technology is actually having a

presentation is it later today or

tomorrow already did it and chris has

already spoken to so there was a session

on that

but-but-but-but

oh it's recorded Oh maybe they are so I

don't know but but but I would say yes

there are definitely some standards

efforts in place that are meant to

address that obviously you know if a

country like the United States China

Russia Israel or a few others really

want to hack a system just candidly

there's not a darn thing you can do

they're gonna do it um just get over it

I I think I think the I I think what the

standards are trying to do is limit the

the number of potential sources of those

type of attacks right and I think you

know we have to measure security as a

risk management process not a not a not

a there's never going to be a risk

process right so I think this thing just

took all the questions away from me oh

wait there it is it went to a poll I

guess so there's a question here

can anyone on the panel's share a good

example of IOT solutions using security

by design oh I'm sorry I'm just trying

I'm trying to I'm trying I'm trying to

there were just a lot more questions

than we expected Oh are there someone at

the mic oh I don't want to like dissuade

anyone from walking up to the mic I just

can't see it I'm blinded by the light as

Bruce Springsteen would say the

[Music]

in a few words can you describe what

companies who are working with IOT can

do to defend themselves so I assume this

is a vendor question about what can

vendors do to defend themselves against

liability when they screw up right you

want to go for it so defend these

lawyers you both take 30 seconds of

piece right so I think there are two

types of companies they're companies

that are being attacked and the

companies that don't know they're being

attacked there isn't any such thing as

every company in the world there isn't

any other thing so you have to go

through a framework again it's down to

getting the holistic viewers to what

you're looking at people process

technology and I like the way he phrased

it it is risk management it's it's

something you do on a constant basis

it's something you you look at on a on

an evolutionary basis and they are going

to be new things there but there's just

so many technologies as long as you have

framework process and a and a way to

follow that process and use the

technologies that exist today I think we

have a lot of solutions there in the

market we need to know what we are

solving for I think you answered it all

right there's a great one here add one

thing to that I think that the

cloud-based security that says for

example you guys offer has the

scalability and the you know that is

really important so once there's X

attacking in retail it can be scaled out

to every single vertical in the same

solution so that it it helps all of you

know the externalities as it were this

is this is a great one how do you assure

they're all great they how do you assure

wrong one yes basically it's a question

about how to restore functionality so

we've talked a lot about you know things

to stop cybersecurity I read this

question has what do you have in place

how do you put plans in place for

restoration after you're taking down

Allison so for that it's slightly

different response because I wanted to

get this in because I think it's

important to also understand that the

smart cities out there they need to when

they're working well they don't need to

work from scratch with regards to them I

because other cities and we're seeing

this more sharing of best practices

across the board from one city to the

next so New York City is in fact

developed a whole series of IOT

guidelines that they are you know and

member cities have signed on to them

they cover security and privacy and data

sharing etc so you don't have to start

from scratch with that so in a way

you're ahead of the game and I just

wanted to make sure we didn't miss that

missed that as part of discussion that's

a great point but does any want to try

this that yeah I think this resilient

cities yes the Brazilian so I'll give

you an example from a Brazilian customer

that we had they said that they deployed

X amount of devices and they see like

two times the devices connect to their

network so they know that half of these

devices are our fake somebody create

them and connect through their network

but they cannot distinguish between the

real one and the fake one because they

didn't have any hardware as you said

route of trust to say which one so now

they have the dilemma of okay if I

disconnect these devices I don't know

which one is the clone I hurt my

customer however if I don't or I let it

connect then I know that I have someone

that is connecting to the net my network

that is doing something bad what do I do

so for example if as you said for the

question as renewability if I can and

this is part of our solution and other

companies are also doing it if I can add

a push of a button renew all the

certificate reset the device remotely

patch them and bring them up again

without having a technician going today

to the sewage as you said right you fix

it then this is a solution that can be

recovered and then I can get rid of all

these cloned devices and now I'm back in

business without a lot of consequences

on like taking my service down for like

days until I fix all the devices

fantastic so there's there's one more

here I I'm sorry if I want to answer

this one it says maybe because this

topic is too complex so can we treat

security using cloud services as an

alternative in order to minimize this

topic I will tell you yes

ask anyone on the panel who disagrees

with me to disagree but I will just say

I have run some of the largest IT

organizations in the world and I would

never take this in-house not on a bet

not not even I wouldn't even consider it

I would always do this in the cloud but

but and there's so many good cloud

platforms and I'm not gonna start naming

them but there are there are half a

dozen world-class IOT platforms out

there almost all the top 12 software

publishers have a platform and then

there's a lot of specialty platforms so

I absolutely does anyone disagree with

that just add that you know my my area

of focus is looking at law enforcement

Public Safety and they have to be you

know some of the most risk adverse

agencies out there and even they are

flocking at the cloud now because they

know that the vendors have you know been

doing cartwheels and hurdles for years

to try to get those security standards

in place and they're there now and they

trust it even more than you know your

on-prem solutions I think yes as long as

in the cloud platform you don't have

your username is admin and password as

that's the only condition you have to

have the people in process to couple it

up with the technology but yes your

cloud service is the way to go yeah I

think it agree the clients IDs are

people and processes issue fundamentally

who's managing that about that platform

and we see that can even get that wrong

still I mean you know records do do tend

to get leaked and so forth but there's a

lot of learning there that can be can be

built upon I think principally with IOT

the main vulnerability for my

perspective lies in the end devices the

end points the things are physically

embedded out there in your cities

they're they're kind of easiest things

things that attack you can physically

get hold of one of these devices take

them apart look at how they work get

into interfaces that they shouldn't get

into reverse-engineer it and then apply

that attack multiple times so to me the

biggest challenges is really focused on

the endpoint devices how you secure

these devices and again that comes back

to a lot of the the points of you

mentioned earlier about you know bedding

secure identity or it all stems back

fundamentally it's fundamental point

secure identity what is that device if

you can't establish the identity you

came over you can't do educated

authentic 18 you know so so is that

that's the kind of tip of the iceberg

and then it builds down to

authentication and so forth so I don't

know how this works whether they

actually come out and hook us or what

but there were not there was not a

single question in here about

distributed ledger technology and I know

some people raise their hand that said

they wanted to hear more about it but no

one actually went up to the mic and ask

the question about it so one last chance

I mean there's a mic there's an open mic

you can you can kind of like hand signal

me are there any questions we haven't

answered that someone really wants

answered run up and grab the mic

otherwise this thing is telling me that

we have to get off the stage but I'm

sure I don't want to put everyone on the

spot but I'm sure we'd all be happy to

go to the side of the room and answer

any questions people have or sit outside

the door and answer questions people

have and I could talk about geeky I

think everyone on here could talk as

geeky as you want about distributed

ledger technology blockchain or Fisher

Merkle trees or whatever floats your

boat other than that I I thank everyone

for coming and I hope you found this

session useful and come by one of their

exhibits or the USA Pavilion and and

talk to us and and we're all happy to

help in any way we can thank you

[Applause]