; 06/04/13 4:54 PM
;
;;;;NEOTECH

;
;
; 06/04/13 4:05 PM
;
;;;;neotech panel 3
;;;;file is: ftc_130604_03

>> ALSO, IT IS ABOUT TO, YOU
KNOW, IT'S ABOUT MAKING,
THOSE ARE THE TWO GOALS, BUT
THAT IS NOT THE GOAL OF MY
TALK.
AND I'M GOING TO SPEAK ABOUT
WHAT I SEE IN TERMS OF THE
MOBILE DEVICES.
WITH AN EMPHASIS ON MALLWEAR
BUT NOT SOLE EMPHASIS
BECAUSE THINGS FLOW INTO
EACH OTHER AS YOU KNOW.
SO FIRST OF ALL, THE
QUESTION IS MALWARE THE SAME
AS -- -- AND COMPUTER
SCIENTISTS-- IT TURNS OUT
BOTH ARE WRONG, OF COURSE.
KNOWN IN THE CONTEXT OF
THREATS LIKE THIS IS NOT
JUST A COMPUTER.
IT HAS MORE RESTRICTED USER
INTERFACE, FOR EXAMPLE, IT'S
HARDER TO TYPE LONG PASSWORDS.
IT HAS A SCREEN THAT IS SUCH
A PRECIOUS THING THAT WE
ALLOW SCROLLING AWAY, AND
ADDRESS BARS WHICH OF COURSE
MEANS IT'S HARDER FOR THE
CONSUMER WHO DO CARE ABOUT T
NOT THAT THERE ARE SO MANY
WHO WANT TO SEE WHERE ARE
THEY ACTUALLY GOING.
IT'S HARDER FOR THEM.
BECAUSE I CAN SCROLL OFF.

I CAN HAVE AN APP OR WEB APP
THAT IS A VICIOUS ONE THAT
IT SCROLLS OFF THE ADDRESS
BAR AND COULD EVEN REPLACE
IN THE CONTENT PORTION AND
SAY BANK OF AMERICA,
WHATEVER YOU WANT.
AND IT MAKES MUCH HARDER FOR
THE END-USER TO KNOW WHERE
THEY ARE AND WHY.
THOSE ARE NOT THE ONLY WAYS
IN WHICH MALWARE AND MOBILE
MALWARE ARE DIFFERENT, OF
COURSE, THERE ARE
LIMITATIONS ON POWER, FOR
EXAMPLE, WHERE THE SMALL
BATTERY DOES NOT COMPUTE ALL
THE TIME WITH RESTRICTIONS
ON HOW TO PATCH, YOU CAN'T
EXPECT FOR THINGS TO BE
FIXED QUICKLY.
AND SO WE'RE FACING AN
ENTIRELY DIFFERENT
SITUATION.
AND THIS DOESN'T EVEN TAKE
INTO CONSIDERATION HOW
PEOPLE USE THIS DEVICES.
I'M GOING TO TOUCH ON THOSE
THINGS.
BUT FIRST I WANT TO TALK A
LITTLE BIT OF WHAT I THINK
THE PROBLEM IS.
THIS IS SOMETHING WE OFTEN
FORGET.
I WANT TO TALK ABOUT WHO IS
ATTACKING 1K.
>> IT'S VERY MARRED TO TALK
ABOUT THINGS IN A MEANINGFUL
WAY.
SO THESE ARE THE THREE
THREATS AS I SEE THEM.
-- JAIL BREAK, TROJANS AND
I'M GOING TO ARGUE THAT
THESE ARE NOT AT ALL THE
SAME.
AND WE CANNOT GROUP THEM

INTO ONE BUNCH.
SO FIRST OF ALL,-- AND
TROJANS ATTACK USERS.
WHEREAS JAILBREAKS TYPICALLY
ATTACK SERVICE PROVIDERS.
THE SERVICE PROVIDER, FOR
EXAMPLE BEING A CONTENT
PROVIDER, A JAILBREAK COULD
MAKE TETHERS FOR SERVICE
POSSIBLE TO THE END-USER AND
COULD ALLOW ACCESS TO APPS
THAT ARE NOT DESIRABLE BY
THE CARRIER.
OR MAYBE THAT AREN'T
DESIRABLE BY THE END-USER.
JUST THAT THEY DON'T KNOW IT.
THEY'RE DIFFERENT IN TERMS
OF HOW THEY GET IN THERE.
-- AND JAILBREAKS OF COURSE
RELY ON PRIVILEGED
ESCALATION.
IN OTHER WORDS, TECHNICAL
VULNERABLE WHEREAS TROJANS
IS BASED ON USER ACTIONS.
AND ABOUT SOCIAL ADHERING
AND THINGS IN THE
MARKETPLACE.
NOW THAT DOESN'T MEAN, OF
COURSE, THAT YOU CAN'T
HAVE-- AND JAILBREAKS THAT
START OUT USING SOCIAL
ENGINEERING BUT THAT'S NOT
THE SOLE WAY OF GETTING ON
THE DEVICE.
AND THERE'S ALSO A BIG
DIFFERENCE IN TERMS OF WHY.
-- DO IT FOR THE MONEY OR
ESPIONAGE DEPENDING ON WHO
IS BEING ATTACKED.
JAILBREAKS ARE ABOUT
CONTROLLING, PIRACY.
THE USER WHO WISHES TO
CONTROL HIS OR HER DEVICE,
PARTICULARLY HIS, I THINK,
AND WHO WISHES TO USE IT FOR
THINGS THAT ARE NOT

ACCEPTABLE BY THE PROVIDERS.
AND TROJANS, THE MAIN REASON
IS GETTING ACCESS TO
INFORMATION.
AND REALLY THE WORST CASE
THERE IS TO GET ACCESS TO-- IN
THE CONTEXT OF FINANCIAL
SERVICE PROVIDERS, THAT IS
THE WORST CASE SINCE THEY
OFTEN RELY ON-- SO ANYBODY
WHO SUBSCRIBES TO-- CAN
THEREFORE READ THOSE AND USE
IT IN ORDER TO GET ACCESS.
SO I ARGUE THESE ARE VERY
DIFFERENT ANIMALS AND IF WE
TREAT THEM AS THE SAME,
WE'RE DOING OURSELVES A BIG
DISFAVOUR.
AND IN PARTICULAR, IF WE
GROUP IN OTHER THINGS LIKE
FISHING AND SCAMS AND THINGS
LIKE THAT AND CALL THEM
THREATS.
-- TO THOSE WHO NEED TO KNOW
WHAT THEY ARE ABOUT.
SO I WOULD LIKE TO MAKE THAT
THEY'RE VERY HONEST WERE
WHAT THE THREATS ARE ABOUT.
NOT TO SAY THAT ONE IS MORE
IMPORTANT THAN THE OTHER.
BUT TO DISTINGUISH AND MAKE
SURE WE UNDERSTAND WHAT ARE
THE THREATS BEING ADDRESSED.
SO NOW A FEW MORE WORDS
ABOUT WHOM ARE BEING
ATTACKED.
IN SOME CASES, JUST ANYBODY.
IN THE CONTEXT OF CLICK
FRAUD, FOR EXAMPLE, IT DOES
NOT MATTER TO THE ATTACKER
WHO THE VICTIM IS OR IN THAT
CASE WHO THE PERSON WHOSE
DEVICE IS BEING INFECTED.
THAT IS NOT NECESSARILY THE
VICTIM BUT IT IS THE
ADVERTISER IN THAT CASE.

THE SECOND POSSIBLE TARGET IS ANYBODY WITH FINANCIAL ACCESS SO IT DOESN'T MATTER WHETHER IT'S YOU OR IT'S ME AS LONG AS IT'S AGO-- YOU OR I HAVE ACCESS TO A FINANCIAL SERVICE PROVIDER AND HAVE SOME REASONABLE AMOUNT OF MONEY IN THE ACCOUNT.
THE ATTACKER COULDN'T CARE LESS.
THEN THERE ARE PEOPLE WITH ACCESS TO A PARTICULAR RESOURCE.
SO FOR EXAMPLE, IF YOU ARE FAMILIAR WITH THE CASE IN WHICH RSA WAS ATTACKED SOME TIME AGO BY NOT JUST MAL WARE BUT BY PEOPLE GAINING ACCESS TO SOCIAL ENGINEERING, THEY WANT AN ACCESS TO SERVERS IN ORDER TO GET ACCESS TO INFORMATION HELD BY THE SERVERS, SO THEREFORE IT'S NECESSARY TO GET TO THOSE PEOPLE AND SO THIS IS SOCIAL ENGINEERING THAT IS TARGETED.
SO YOU'VE GOT VERY TARGETED PERSON.
IF YOU WANT THE PERSON WHO HAS A PARTICULAR KIND OF INFORMATION OR A PERSON INTERESTED TO AN ORGANIZATION, IT'S THAT PERSON, NOBODY ELSE.
>> AND AS A LAST ONE, AN ORGANIZATION.
IF YOU WISH TO EITHER CAUSE LOSS OF MONEY TO AN ORGANIZATION OR GET ACCESS TO RESOURCES, INFORMATION TO AN ORGANIZATION, IT DOESN'T QUITE MATTER WHO WE GET IT FROM AS LONG AS WE HAVE THE PRIVILEGES OR MEANS TO THE

DESIRED RESULT.
AND SO IF WE DON'T
DISTINGUISH ABOUT WHO ARE
BEING ATTACKED, AGAIN WE'RE
FORGETTING SOMETHING
IMPORTANT HERE.
SO THESE ARE ALL
CONSIDERATIONS WORTHWHILE.
>> NOW I WOULD ALSO ARGUE
THAT IF YOU CAN UNDERSTAND
WHAT'S HAPPENING, PREDICT
WHAT IS GOING TO HAPPEN,
THIS IS NOT ONLY FROM THE
PERSPECTIVE OF WHAT THE
COSTS ARE AND THE TECHNICAL
DIFFICULTY ITS IN ORDER FOR
THE PARTICULAR ATTACK BUT
ALSO SOCIAL ENGINEERING
ABOUT JUST HOW GULL I
BELIEVE ARE PEOPLE IN THE
CONTEXT OF A PARTICULAR
ATTACK AND HOW EASY IS IT IS
FOR THEM TO GET IT AND YOU
COULD THINK ABOUT THAT AS
NOT THEIR PEAK ABILITIES BUT
THEIR AVERAGE ABILITIES TO
AVOID BEING ATTACKED.
AND IF THAT IS RATHER LOW
THEN YOU'VE GOT A GOOD
OPPORTUNITY.
WHEREAS IF IT'S-- THERE'S
LESS.
SO UNDERSTANDING THE SOCIAL
VULNERABLE IS ALSO HELPFUL
IN ORDER TO UNDERSTAND WHERE
ARE THE ATTACKERS GOING TO
COME FROM.
THE ATTACKERS ARE GOING TO
GO WHERE IT'S MOST-- SO IF
YOU COULD IDENTIFY THE PLACE
THAT IS MOST FREE, WHETHER
IT'S THE EASIEST, THE MOST
DESIRABLE FROM A FINANCIAL
PAYOFF POINT OF VIEW, OR THE
WAY IN WHICH THEY'RE MOST
DIFFICULTY TO BE BOOTED OUT

THOSE ARE THE WAYS IN WHICH
WE COULD CLASSIFY AREAS.
SO IT'S IMPORTANT FOR US IF
WE WANT TO PREDICT WHAT IS
GOING TO HAPPEN NEXT TO
UNDERSTAND FROM THE
PERSPECTIVE OF ALL OF THESE
ASPECTS THAT I DESCRIBED
WHERE IS THE DESIRE.
AND IF WE DON'T, WE ADDRESS
THE WRONG PROBLEM.
ONE PARTICULAR ENTITY THAT
IS OFTEN FORGOTTEN IS THE
END-USER.
IT IS AMONG TECHNICAL PEOPLE
AND THE TECHNICAL PEOPLE IN
THIS ROOM THEY THINK OF
MALWARE THAT IS SOMETHING
STRICTLY TECHNICAL AND IT
DOESN'T HAVE ANYTHING TO DO
WITH THE END-USER.
IF WE DON'T TAKE THE
END-USER INTO CONSIDERATION
WE'RE MISSING AN IMPORTANT
PART OF THE EQUATION.
SO THIS IS A GRAPH THAT YOU
COULD IMAGINE IS THE
PROPAGATION GRAFT OF MALWARE,
IT ISN'T IT TURNED OUT THE
PROPAGATION OF A HUMAN BORN
VIRUS AND THE REASON I TOOK
THIS IS BECAUSE WE KNOW MUCH
MORE ABOUT HUMAN BORN
VIRUSES THAN COMPUTER
VIRUSES IN SPITE OF THE FACT
THAT IT SHOULD BE SO EASY
FOR US TO MEASURE MALWARE.
IT'S JUST VERY HARD TO GET
TO EVEN WHEN YOU WORK IN A
LARGER-- AND THE WITHIN IS
SIMPLE.
HUMAN BORN VIRUSES DON'T TRY
TO HIDE.
MALWARE TRIES TO HIDE, TRIES
ITS BEST TO HIDE AND THERE
ARE LOTS OF UNINTENSES

CONSEQUENCES.
BUT ANYWAY, BACK TO THE USER HERE.
THE USER AND THE-- IS VERY IMPORTANT.
IF YOU RUN A DESKTOP READING OF EVERY MORNING AND YOU HAVE AN E-MAIL BORN VIRUS AND YOU MAY AS A RESULT OF THE READING E-MAIL ACTIVATE IT AND HAVING IT BEING PROPAGATED-- NOW THAT IS GOING TO HAPPEN AT A CERTAIN-- WHEREAS IF YOU HAVE ACCESS 24/7 TO A DEVICE, HAND SET, IT'S VERY SIMILAR THREAT BUT WITH 24/7 ACCESS.
OF COURSE-- BECAUSE YOU CAN ACCESS IT FOR OFTEN AND THE PEOPLE RECEIVE THEWAY THE MARKETPLACE REACT TO ITS MALLWARE IS TO DETECT SOMEWHERE ALONG THIS RAMP-UP AND THEN IT TAKES AWHILE TO CHURN OUT AN ANTIDOTE AND THEN TO-- THAT MEANS THAT THE VULNERABLE TIME FROM THE POINT OF VIEW OF THE ATTACKER IS THE RAMP-UP.
ANYBODY WHO WILL-- CAN SPEED UP RAMP UP IS GOING TO BE MORE SUCCESS.
S THIS'S ONE ONE REASON WHY HANDSETS ARE MORE DESIRABLE TO ATTACKERS.
NOW ALSO, I WANT TO MAKE SURE THAT YOU DON'T STICK TO-- ONLY IN THIS DISCUSSION.
IF YOU ARE'S GOING TO PREDICT THE PROBLEM WE SHOULD ALSO THINK ABOUT NONEXISTENT-- FOR EXAMPLE IN GOOGLE DOCS, THERE YOU TRULY HAVE USERS, ONCE IT'S IN THEIR FACE, SORRY FOR THE

PUN, IT IS GOING TO BE MUCH FASTER.
SO WE, IN ORDER TO ANTICIPATE WHERE THINGS ARE MOVING, NOT ONLY WILL YOU HAVE TO LOOK AT THE ATTACK SERVICE FROM A TECHNICAL POINT OF VIEW AND THE SOCIAL RAMIFICATIONS OF TECHNOLOGY BUT ALSO WHERE SOCIAL SPEAKING IN TERMS OF-- AND THAT'S GOING TO BE PORN FOR US IN ORDER TO PREDICT THINGS, SO THIS BRINGS ME TO ONE THING.
WHAT DO PEOPLE WANT.
AND THERE WAS TALK ABOUT THIS MORNING ABOUT WHAT WE SHOULD DO IN TERMS OF COMMUNICATING WITH THE SEARCH AND HOW TO MAKE SURE WE DO THE RIGHT THING THIS IS WHAT USERS WANT ONE BIG BUTTON THAT SAYS MAKE ME HAPPY.
THEY PRESS IT AND THEY GET HAPPY, REALLY.
A FEW YEARS AGO IT WAS VERY COMMON TO PROVIDE USER EDUCATION LIKE FINANCIAL INSTITUTIONS, FOR EXAMPLE, WHERE THE FINANCIAL INSTITUTION SAID MAKE SURE YOU TURN OFF JAVASCRIPT, DON'T USE.
IF AND OF COURSE THAT IS A RIDICULOUS PIECE OF ADVICE IN A WORLD DOMINATED BY JAVASCRIPT.
WE CAN'T DO ANYTHING WITHOUT USING JAVASCRIPT.
SIMILARLY, MAYBE USERS SHOULD NOT BE TOLD TO TURN OFF BLUE TOOTH AND I WOULD FEW BECAUSE IT'S AN INSTRUCTION THAT IS CONTRARY

TO THEIR WISHES, THEY WISH
TO COMMUNICATE AND RECEIVE
INFORMATION.
AND THEY DON'T WANT TO
SWITCH BACK AND FORTH.
THAT IS A COMPLICATIONMENT
THEY WANT THINGS TO BE
TRANSPARENT, AUTOMATIC AND
SAFE.
AND TO THE EXTENT THAT THERE
IS A PROBLEM, THEY WANT TO
BE ABLE TO HAVE THE DAY
AFTER PILL.
SO THAT THEY SAY YOU KNOW,
EVERYTHING IS FINE NOW.
AND TO THE EXTENT THAT IS
POSSIBLE, WE SHOULD TRY TO
PROVIDE THAT.
SO WHEN WE DO COMMUNICATE TO
THE USER, HOW DO WE
COMMUNICATE IT TO THEM.
THIS IS THE EXAMPLE OF THE
TRADITIONAL APPROACH.
ARE YOU SURE YOU WANT TO
INSTALL THE UNSIGNED
APPLICATION NAME, CLICK YES
TO PROCEED IN CAPITALS AND
OF COURSE PEOPLE READ CLICK
YES TO PROCEED AND THEY
CLICK YESMENT NOW THAT'S HOW
WE DEAL WITH SECURITY.
NOW WHAT WE SHOULDN'T DO IS
SAY DRIVE THE SKULL TO THE
COMPUTER TO THE COMPUTER TO
INSTALL AND TO COMMUNICATE
THAT THIS IS NOT A GOOD
THING TO DO AND YOU DON'T
WANT TO DO THIS AND ARE YOU
REALLY GOING IT TO DO IT
ANYWAY, THEN ARE YOU ON YOUR
OWN.
SO IN ORDER TO DISTINGUISH
BETWEEN-- WE NEED TO FIRST
OF ALL KNOW WHAT THE THREATS
ARE AND THEN TO THE EXTENT
THAT IT'S POSSIBLE AND

MEANINGFUL TO COMMUNICATE WE
NEED TO DO SO WHEN IT ISN'T
MEANINGFUL TO COMMUNICATE
AND WE KNOW THIS IS TO THE
DESIRABLE, WE SHOULD SIMPLY
MAKE IT IMPOSSIBLE TO
PURCHASE.
NOW THERE A BUNCH OF
TECHNICAL APPROACHES.
YOU HAVE HEARD ABOUT MANY OF
THEM THIS MORNING.
EVERYBODY UNDERSTANDS HOW
DATA EXECUTION PREVENTION IS
WORKS AND YOU COULD DO CODE
SIGN AND CODE OBFISCATION,
THIS IS GOOD TO MAKE IT
HARDER.
FILTERING IN THE MARKETPLACE
IS GREAT.
NOW THAT PROTECTS AGAINST
SOME FORMS OF ATTACKS BUT
NOT ALL.
AND IN PARTICULAR IT DOESN'T
PROTECT AGAINST
ATTACKS-- AND YOU CAN FILTER
DURING RUNTIME ON THE DEVICE
WHICH IS TRADITION
ANTI-VIRUS APPROACH.
SIGNATURES BEHAVIORAL
APPROACHES WHICH ISN'T THE
GREATEST ON A DEVICE WITH
LIMITED BATTERY POWER OR DOT
SAME THING ON THE WEB.
AND INSTEAD LOOK FOR ACCESS
TO CONTROL CENTERS AND LOOK
AT THE VELOCITY IN WHICH
THINGS SPREAD AND SO ON OR
YOU COULD AUDIT BEFORE
ANY-- AND THAT'S SOMETHING
THAT I BELIEVE IS HELPFUL TO
SAY YOU'RE ABOUT TO ENTER
YOUR BANK -- WE'RE STARTING,
NOW WE'RE GOING TO CHECK.
>> AND OF COURSE AS WELL YOU
COULD PATCH.
AND THIS IS A NATURAL THING

TO DO.
WHEN YOU NOTICE SOMETHING THAT ISN'T SO GOOD, THEN YOU PATCH.
NOW UNFORTUNATELY PATCHING IS COMPLICATED AND NOT SO AFFORDABLE.
AND IT COMES WITH ALL KINDS OF TECHNICAL COMPLICATIONS BECAUSE THE NUMBER OF VERSIONS OUT THERE.
SO THESE ARE NOT SAYING THAT ONE IS BETTER THAN THE OTHER BUT THEY COMPLEMENT EACH OTHER BUT WE SHOULD UNDERSTAND THAT THESE ARE TECHNICAL APPROACHES, THEN WE HAVE TO CHOOSE.
>> NOW THE QUESTION IS WHO CARES.
FIRST OF ALL WE HAVE USERS.
THEY WANT THEIR SIMPLE LIFE.
YOU HAVE RI LYING PARTIES.
THEY WANT TO AVOID LOSSES.
GOVERNMENT WANTS TO CONTROL CRIME.
CARRIERS WANT TO AVOID LOSSES, OF COURSE, AT THE SAME TIME SELL SERVICES AND THE OEMS WANT TO BE COMPETITIVE AND SELL SERVICES.
NOW WHY DO WE RELY ON THOSE MOST.
THAT IS WHO CARES AND WHY, THAT IS A REALLY UNFORTUNATE SITUATION.
WE NEED TO START PROVIDING SECURITY THAT ISN'T NECESSARILY DEMANDED BEFORE THEY SUPPLY IT.
USERS DON'T KNOW THEY CAN HAVE THE SECURITY UNTIL WE PRESENT THIS TO THEM.
AND THE QUESTION OF WHERE THE FOCUS SHOULD BE.

YOU HAVE TODAY'S THREAT
WHICH I REPRESENT BY THIS OR
TOMORROW'S THREAT AS IT
COULD TURN OUT.
WE NEED TO LOOK AT BOTH.
IF WE ONLY FOCUS ON THE EGG,
THEN WE ARE REALLY FOOLING
OURSELVES.
AND NOW IN ORDER TO GET
CONTEXT FOR MY BELIEFS, I AM
SPEAKING AS A REPRESENTATIVE
OF FATSKUNK WHICH IS A
SOFTWARE COMPANY THAT ALLOWS
A TESSTATION OF DEVICES TO
DETERMINE THAT THE DEVICE
ISN'T INFECTED.
IT'S BASED ON PHYSICS.
IT'S NOT BASED ON PATCHING
OR DETECTING CODE.
IT IS JUST SAYING THERE IS A
PIECE OF CODE RUN ON THE
DEVICE.
AND THEREFORE SINCE THE
OPERATING SYSTEM TO ALL
ROUTINES TO STOP EXECUTING
THIS, IT MUST BE BAD.
AND SO THAT IS
NONTRADITIONAL APPROACH.
AND IT COULD BE USED, FOR
EXAMPLE, TO DETERMINE THAT
ENVIRONMENTS ARE TRULY TO BE
TRUSTED BUS TODAY WE ARE
RELYING ON CODE HARDENING
AND CODE SIGNING, THINGS
LIKE THAT, WHICH WE KNOW ARE
DESCENT BUT AREN'T FOOLPROOF.
AND SO WHAT I BELIEVE HAS TO
BE DONE IS TO UNDERSTAND ALL
THE ATTACKS AND ALL
THE-- AND THEN FIGURE OUT
HOW TO PUT THEM IN CONTEXT.
AND THAT CONCLUDES MY
PRESENTATION.
ANYBODY HAS A QUESTION, I'M
VERY HAPPY TO ANSWER.
THANK YOU SO MUCH.

(APPLAUSE)
I SHOULD HAVE MENTIONED AT THE ON SENT THAT HE IS ALSO PARTICIPATING IN THE PANEL. SO YOU CAN ASK QUESTIONS OF THAT TYPE AS WELL.
ALL RIGHT.
SO ONCE AGAIN MIME NAY IS PAUL.
THANK YOU VERY MUCH FOR JOINING US TODAY, I HAVE LEARNED A TON ALREADY AND IT'S BEEN A REALLY, REALLY INTERESTING MIX OF PEOPLE.
BEFORE I BEGAN I WANTED TO GIVE YOU TWO OF THE GROUND RULES WE ALREADY TALKED ABOUT TODAY.
FIRST, PLEASE FIND THE LITTLE QUESTION CARDS, THEY'RE STILL FLOATING AROUND, THEY'RE STILL IN YOUR FOLDER, THAT IS ONE WAY TO GET A QUESTION TO ME AS THE MODERATOR AND I WILL TRY AND DO IT JUSTICE.
WE'RE ALSO GETTING ALOT OF QUESTIONS THROUGH TWITTER SO HI, THOSE OF YOU, WHO ARE DOING NOTHING BUT WATCHING A WEBCAST ALL DAY, TO THE DOING YOUR WORK.
WE'RE GLAD FOR YOUR DERELICTION BECAUSE IT HAS BEEN A LOT-- HAD A LOT OF REALLY INTERESTING QUESTIONS.
THE SECOND THING I WANTED TO SAY AT THE OUTSET WHICH HAS BEEN SAID BEFORE IS WE DONE HAVE THE TIME AND WE'RE NOT USING THE TIME TO GO THROUGH THE LONG AND IMPRESSIVE BIOS OF EVERYONE THAT WE INVITED.
I REALLY DO URGE YOU TO AT SOME POINT DURING A BREAK,

STUDY THE BIOS OF THESE
PEOPLE.
THEY'RE REALLY IMPRESSIVE.
ON THIS PANEL IN PARTICULAR
WE DECIDED THAT YOU HAD TO
BE NAMED ALEX OR JOHN TO
PARTICIPATE.
SO WHEN I ASK QUESTIONS IF I
JUST SAY ALEX AND HOPE THAT
ONE OF THEM HAS SOMETHING TO
SAY ABOUT THIS.
BUT I DID WANT TO BRIEFLY GO
OVER ALEX GANTMAN FOR
QUALCOMM, JOHN MARINHO AT
CTIA AND BY THE WAY YOU SAW
JUSTICE SCALIA'S SNARK ABOUT
THE CTIA IN THE LAST WEEK.
WE CAN TALK ABOUT THAT
LATER.
THAT MADE NO SENSE.
JON ONERHEIDE, CHIEF
TECHNOLOGY OFFICER FOR DUO
SKIRT BUT REALLY HAS WORN
MANY HATS IN THE HOB IL
SECURITY SPACE AND ALEX RICE,
FROM FACEBOOK.
HERE IS THE SET UP.
AT ONE POINT WE WERE GOING
TO HAVE SHALL DID -- SORRY,
AT ONE POINT WE WERE GOING
TO HAVE WHAT WE WERE CALLING
THE INDUSTRY PANEL.
AND THISES WITH GOING TO BE
MEMBERS OF THE MANY PIECES
OF THE COMPLEX MOBILE
ECOSYSTEM THAT STEVE STARTED
OUR DAY WITH.
AND FRANKLY WE HAD THIS RARE
EVENT, THIS EMBARRASSMENT OF
RICHES WHERE MANY, MANY,
MANY DIFFERENT PEOPLE AGREED
TO PARTICIPATE.
IT'S A NICE PROBLEM TO HAVE.
AT ONE POINT WE REALIZED
WELL, THE SOLUTION HERE IS
TO BREAK THAT PANEL INTO

TWO.
AND A NATURAL LINE SEEMED TO BE LET'S HAVE ONE PAN WELL ALL OF THE PLATFORM PEOPLE.
THE QUESTIONS WILL BASICALLYLY BE FAIRLY UNIFORM TO A BUNCH OF PEOPLE WHO ASK AND ANSWER THE SAME QUESTIONS.
AND THEN AFTER WE'VE ABSORBED AND LEARNED WHAT THEY DO, WE'RE GOING TO INVITE OTHER PEOPLE WHO REPRESENT A WHOLE PANOPLY OF DIFFERENT POSITIONS IN THE ECOSYSTEM TO MAKE THINGS COMPLEX, RIGHT, TO TAKE THOSE LESSONS AND THEN BUILD ON.
SO THAT'S WHAT WE'VE TRIED TO DO.
NOW THAT IS A TOUGH THING TO DO A LITTLE INCOMPLETE.
YOU NOTICE WE DON'T HAVE A COMPANY THAT DOES FOG BUT BUILD HANDSETS.
YET WE DO HAVE THE CTIA WHO HAS MANY OF THEM IN THEIR MEMBERSHIP.
WHAT WE WANT TO DO WITH THIS ONE IS REALLY TALK ABOUT THE REST OF THE ECOSYSTEM PUT THE PARTS IN MOTION.
THAT IS MY FIRST QUESTION, OH, NO, ACTUALLY, TAKE THAT BACK.
JOHN MARINHO OF CTIA AND BY VIRTUE OF HAVING A MEMBERSHIP THAT REPRESENTS TWO-THIRDS OF THAT ECOSYSTEM, MAYBE MORE, WE THOUGHT WE WOULD INVITE HIM TO SPEND A FEW MINUTES WITH A FEW SLIDES TALKING ABOUT KIND OF HIS REFLECTIONS ON THE EARLY MORNING.
I SAID YOU SHOULD DO IT FROM

YOUR CHAIR BUT I THINK YOU
NEED TO BE STANDING TO
ADVANCE THE SLIDES.
LET ME MAKE SURE-- THESE ARE
THE RIGHT SLIDES, RIGHT.
OKAY.
SO JOHN, TAKE IT AWAY.
>> THANKS, PAUL, REALLY
APPRECIATE IT.
SO AGAIN, GOOD AFTERNOON,
LADIES AND GENTLEMEN.
MY NAME IS JOHN MARINHO WITH
CTIA AND I'M GOING TO FIRST
OF ALL THANK PAUL AS WELL AS
THE FTC FOR THIS OPPORTUNITY
BECAUSE I HAVE TO SAY THAT I
HAVE REALLY ENJOYED THE
MORNING.
IT WAS A GREAT SET OF
PANELS.
AND IN FACT THE SPEAKERS
HAVE MADE JOB A LOT EASIER
WITH REGARDS TO THIS PART OF
THE AGENDA.
SO I PROMISED PAUL I WOULD
KEEP MY COMMENTS VERY BRIEF.
AND SO IN THE SPIRIT OF THAT
LET ME BEGIN BY FIRST
HIGHLIGHTING SOME WORDS THAT
KIND OF STRUCK ME AS WE
LISTENED IT TO THE PANELISTS
OF THIS MORNING.
BECAUSE WE HEARD WORDS LIKE
STATIC ANALYSIS, DYNAMIC
ANALYSIS, SOCIAL ENGINEERING,
POLYMORPHIC AND MET MORPHIC,
MALWARE, JAILBREAKS, ROOTKITS,
CHIPS,-- A SERIES OF
STATISTICS ABOUT THE MALWARE
INFECTION RATE IN THE UNITED
STATES FROM AS LITTLE AS
1/10,000 OR LESS TO
SOMETHING ON THE ORDER OF
2%.
INDEED, WE HEARD AND SAW
WHAT THE LAYERING EFFECT IS

OF THE MOBILE ECOSYSTEM, PARTICULARLY AS DESCRIBED IN THE LAYER OF TERMS THAT I REALLY ENJOYED.
BUT INDEED, ONE OF THE KIND OF INTERESTING THINGS WHEN YOU REFLECT UPON ALL OF THAT, IS THAT WE'RE DEALING WITH COMPLEXITY.
WE'RE DEALING WITH A VERY DYNAMIC ECOSYSTEM, AN ECOSYSTEM THAT IS VERY RICH AND ROBUST.
WE'RE DEALING WITH AN INDUSTRY THAT IS ACUTELY FOCUSED ON THE IMPORTANCE THAT SECURITY HAS TO DEAL WITH.
SO THAT TO ME REALLY STRUCK ME FROM THIS MORNING AS A GREAT STORY, PARTICULARLY WHEN YOU LOOK AT THE DIVERSITY OF PLAYERS THAT WE SAW AGAIN ON PANEL NUMBER 2, WHEN YOU LOOK AT THAT PARTICULAR DIALOGUE, AS WELL AS EVEN BEFORE THEN IN TERMS OF ALL OF THE COMPLEXITIES THAT WE'RE DEALING WITH.
SO THE GOOD NEWS IS THAT THE INDUSTRY IS FOCUSED.
9 ECOSYSTEM IS FOCUSED ON DOING THE RIGHT THING FOR THE END-USER AND THE GOOD NEWS IS IT SEEMS TO BE PAYING OFF IN TERMS OF MALWARE INFECTION RATES AND I WILL TALK ABOUT THAT AS WE GO THROUGH THE MATERIAL.
SO INDEED, MOBILE SKOOIB SECURITY-- CYBERSECURITY IS A TOP PRIRT AND I THINK WE SAW THAT FROM ALL THE SPEAKERS THIS MORNING AND WILL REINFORCE THAT.
WE HAVE OVER 250 MEMBERS.

WE HAVE CREATED A
CYBERSECURITY WORKING GROUP.
THAT WORKING GROUP HAS
REPRESENTATIVES FROM ALMOST
EVERY ELEMENT OF THE
ECOSYSTEM INCLUDING THE
PLAYERS THAT YOU SAW ON
PANEL NUMBER TWO AS PART OF
THE CYBERSECURITY WORKING
GROUP.
AND IT PROMOTES AN OPEN AND
DIVERSE ECOSYSTEM WHICH IS
GIVEN US 150 MILLION SMART
PHONES IN THE UNITED STATES
AND GROWINGMENT AND GROWING
VERY, VERY RAPIDLY.
SO WHAT'S THE KEY TO
CYBERSECURITY.
I LIKE TO DESCRIBE IT AS A
TEAM SPORT.
EVERYBODY HAS A VESTED
INTEREST IN INSURANCING THAT
CYBERSECURITY IS ADDRESSED
REGARDLESS OF WHETHER YOU
ARE PROVIDING AN OS, AN
APPLICATION, WHETHER YOU'RE
PROVIDING A SERVICE, WHETHER
YOU'RE PROVIDING A DEVICE,
INDEED EVERYBODY HAS A
VESTED INTEREST IN A HIGHLY
COMPETITIVE MARKET IS SO
THAT IS AN IMPORTANT
ATTRIBUTE TO KEEP IN MIND.
INDEED THERE IS NO QUICK FIX
TO CYBERSECURITY.
OFTEN WHI I TALK TO FOLKS ON
THE HILL OR IN DIFFERENT
GOVERNMENT AGENCIES THEY
ALWAYS ASK, ISN'T THERE A
LOCK YOU COULD PUT ON THE
DOOR.
AND UNFORTUNATELY THERE
ISN'T.
BECAUSE YOU ARE REALLY
DEALING WITH SOMETHING MUCH
MORE COMPLEX THAN JUST A

SIMPLE LOCK ON A DOOR.
AND I LIKEN IT TO THE
ANALOGY OF A HOUSE IN THE
SENSE THAT A HOUSE HAS MANY
THINGS IMPACTED BY SECURITY,
FROM THE FOUNDATION TO THE
DOORS, THE WINDOWS, THE ROOF,
THE CHIMNY AT TIMES AND
INDEED THERE IS NO CIVIL
BULL ELEVATOR.
YOU HAVE TO REALLY FOCUS ON
ALL THE DIFFERENT ELEMENTS
THAT IMPACT IT CONSUMER
EDUCATION WE HEARD THAT OVER
AN OVER AGAIN AND WE'RE
TRYING TO DO EVERYTHING WE
CAN THROUGH CTIA TO DRIVE
CONSUMER EDUCATION.
YOU'LL FIND THAT ON OUR WEB
SITE, EVERYTHING THAT WE
RECOMMEND FOR CONSUMERS IN
TERMS OF HOW TO BE SAFE
ON-LINE WITH THEIR SMART
PHONE, WE SERIES OF
CYBERSAFETY TIPS, SOME OF
THAT MATERIAL WE BROUGHT
ALONG WITH US AND IT WAS
AVAILABLE ON THE TABLE
OUTSIDE THE MEETING ROOM BUT
INDEED IT IS A FOCUS BECAUSE
YOU CAN'T DICTATE OR MANDATE
THAT PEOPLE HAVE TO PUT
LOCKS ON THEIR DOOR, EVEN
THOUGH IT IS A GOOD IDEA.
AT THE END OF THE DAY
CONSUMER EDUCATION IS
IMPORTANT BECAUSE AGAIN IT'S
A TEAM SPORT.
EVERYBODY HAS A ROLE TO PLAY
INCLUDING THE CONSUMER.
LASTLY I ALWAYS LIKE TO
BRING UP PRIVACY JUST
BECAUSE THEY'RE NOT
DIAMETRIC.
CYBERSECURITY AND PRIVACY.
BECAUSE I LIKE TO DESCRIBE

THAT THE PRIVACY IS ABOUT
WHAT DATA YOU PROTECT AND
CYBERSECURITY ABOUT HOW YOU
PROTECT THAT DATA.
SO THE TWO HAVE TO WORK
HAND-IN-HAND.
AND INDEED, IT SUPPORTS THE
WHOLE NOTION OF THE
ECOSYSTEM, HOW THE ECOSYSTEM
HAS TO WORK COLLABORATIVELY
WHEN IT WORKS, THERE IS
GOING TO BE A TEST ON THIS
IN THE AFTERNOON BUT INDEED
WHAT I TRY TO DO HIRE IS TO
KIND OF REALLY HIGHLIGHT HOW
THE CONSUMERS REALLY AT THE
CENTRE OF OUR DISCUSSION
WHEN IT COMES TO THE
ECOSYSTEM.
BECAUSE THEY'RE INDIVIDUALS,
THEY'RE PROFESSIONALS WHEN
THEY WORK WITH AN ENTERPRISE,
THEY COULD ALSO WORK FOR THE
GOVERNMENT.
BUT INDEED THEY'RE AT THE
CENTRE OF THE ENTIRE
DISCUSSION BUT THERE ARE A
LOT OF DIFFERENT PLAYERS IN
THE ECOSYSTEM THAT TOUCH THE
DEVICE FROM THE APPLICATION
TO LET'S SAY THE AGGREGATORS
TO THE APPLICATION
MARKETPLACE.
I WON'T BOTHER YOU WITH THE
DETAILS BECAUSE WE HEARD A
LOT ABOUT THAT EARLIER TODAY
BUT INDEED THAT'S WHY IT IS
SO IMPORTANT FOR THE
ECOSYSTEM TO COME TOGETHER
AND LOOK AT THE DIFFERENT
THINGS THAT EACH PLAYER
NEEDS TO DO SO YOU CAN
DELIVER ON THE PROMISE OF
SECURITY.
AND IN SOME SENSE MAINTAIN
THE INTEGRITY OF THAT HOUSE

I DESCRIBED EARLIER.
SO WHAT DOES THAT ALL MEAN?
WHAT IT MEANS, IS THAT THE
U.S. HAS ONE OF THE LOWEST
MALLWARE INFECTION RATINGS
IN THE WORLD AND I HAVE TO
THANK THE PREVIOUS SPEAKERS
BECAUSE THEY MADE MY POINT
FOR ME BUT INDEED, JUST TO
COMPARE AND CONTRAST THESE
NUMBERS, IN, AND THIS IS
BASED UPON INDUSTRY REPORTS
THAT WE SCANNED ON THE ORDER
OF ABOUT REPORTS FROM
COMPANIES LIKE SYMANTEC,
TREND MICRO, M T-MOBILE WAS
ONE OF THE REPORTS AN
THEY'RE AMAZINGLY
CONSISTENT.
WHEN YOU LOOK ACROSS ALL
THESE DIFFERENT REPORTS THIS
IS A STUDY WE DID LATE LAST
YEAR.
WHAT YOU FIND IS THAT IN
COUNTRIES LIKE RUSSIA AND
CHINA, MALLWARE INFECTION
RATES ARE IN EXCESS OF 40%.
I WILL REPEAT THAT.
EXCESS OF 40% WHEN IT COMES
TO CHINA THAT'S A REALLY BIG
NUMBER.
THAT'S ON THE ORDER OF OVER
100 MILLION SMART PHONES
THAT ARE INFECTED WITH
MALWARE, BASED UPON NUMBERS
AT THE END OF THE FIRST
QUARTER.
WHEREAS IN THE U.S. AGAIN WE
HEARD FROM PATRICK TRAIN ERR
AND Q MOBILE AND THE NUMBER
IS DRAMATICALLY LOWER.
AND INDEED WE HAVE SOME
INDICATIONS THAT THE NUMBERS
ARE EVEN GETTING BETTER IN
THE FIRST QUARTER, ABOUT
2013.

SO AT THE END OF THE DAY
WHEN WE LOOK AT THESE
DIFFERENT STUDIES WHAT WE
FIND IS THAT THERE ARE TWO
THINGS THAT REALLY DRIVE
THAT.
WHICH IS THAT INDEED THE
INDUSTRY IN THE U.S. IN
PARTICULAR HAS STANDARDS AND
PRACTICES THAT THEY FOLLOW
THERE ARE A WAELT OF
STANDARDS, WE HEARD ABOUT A
LOT OF THEM EARLIER TODAY.
A WEALTH OF STANDARDS BEING
IMPLEMENTED AND THE SECOND
IS KUR RATED APP STORES.
PREVIOUS PANEL TALKED ABOUT
THAT.
THEY ARE KUR RATED IN
DIFFERENT METHODS.
THEY ARE KUR ATED BY
DIFFERENT BUSINESS MODEL ITS
AND APPROACH TO THE
MARKETPLACE BUT AT THE END
OF THE DAY WHEN YOU LOOK AT
THE RESEARCH IF BASICALLY
SAYS THAT INDEED, WITHIN THE
U.S., THE APP STORES ARE
CURATED AND THEN OUTSIDE THE
U.S. THAT IS NOT NECESSARILY
THE CASE.
AND WE SEE THAT IN THE
NUMBERS THAT I MENTIONED
EARLIER.
SO AT THE END OF THE DAY
WHAT I WOULD LIKE TO BRING
UP IS THE FACT THAT THERE
ARE A WEALTH OF SECURITY
SOLUTIONS ACROSS THE MOBILE
ECOSYSTEM BUT THAT DOESN'T
MEAN TO SAY THAT WE'RE DONE
BECAUSE WE'RE NOT.
IN FACT IF YOU GO TO OUR WEB
SITE WHAT WILL YOU FIND IS
MATERIAL THAT TALKS ABOUT
WHAT ARE THE SOLUTIONS THAT

THE INDUSTRY HAS AVAILABLE TODAY.
BUT WILL YOU ALSO FIND A BLUEPRINT IN TERMS OF WHAT ARE WE LOOKING AT THE IN THE FUTURE.
WHAT ARE THE THINGS WE ARE TARGETING BECAUSE WE'RE TRYING TO STAY AHEAD OF THE THREAT, TRYING TO STAY AHEAD OF THE BAD GUYS.
THAT'S PART OF OUR EFFORT AND WHY WE DO RESEARCH.
LASTLY WE LOOK AT MOBILITY IN TERMS OF HOW IT FITS INTO THE BIGGER TRENDS OF THE INTERNET BECAUSE YOU CAN LOOK AT MOBILITY AND ISOLATION BECAUSE AS ONE SPEAKER SAID EARLIER TODAY THERE IS NO DISTINCTION BETWEEN THE MOBILE WEB AND THE WEB.
THEY'RE ONE AND THE SAME.
SO AGAIN I WELCOME THAT YOU VISIT OUR WEB SITE IN THE SUPPLEMENTARY INFORMATION IN MY MATERIAL.
I HIGHLIGHT SOME OF THAT AS WELL AT THE URLs IN WHICH YOU CAN TRY AND TRACK DOWN THAT INFORMATION.
AND YOU'RE ALSO FREE TO CONTACT ME IF YOU HAVE ANY PROBLEM IN GETTING THAT INFORMATION.
SO WITH THAT, PAUL, I WILL TURN IT BACK TO YOU.
>> CAN YOU FLIP BACK TWO SLIDES.
>> SURE.
I THINK THIS IS A GOOD BACKDROP FOR THE FIRST QUESTION.
WITH THE SET UP IN THIS ROOM THE ONLY PEOPLE WITHOUT

CAN'T SEE THE SLIDES ARE
THOSE OF US ON STAGE.
BUT SUFFICE IT TO SAY IT'S A
COMPLICATED MAP OF THE
ECOSYSTEM.
IF ALL YOU FEW ABOUT MOBILE
SECURITY WAS WHAT HE LEARNED
IN THE LAST PANEL YOU WOULD
THINK IT BEGINS AND ENDS
WITH THE PLATFORM, THE
OPERATING SYSTEM DEVELOPER
IN THE CASE OF SOME OF THESE
PLATFORMS, INTERGRATED
COMPANIES THAT DO MORE THAN
ONE THING IN IN ECOSYSTEM.
BUT INDEED THERE ARE LOTS OF
OTHER PLAYERS.
SO THE FIRST QUESTION AND I
WILL START WITH YOU, ALEX,
IS WHAT DO OTHER INDIVIDUAL
PARTS INFORM VERY
COMPLICATED GRAPH, WHAT ARE
THEIR OBLIGATIONS WITH
REGARD TO SECURITY, AND WHAT
ARE SOME EXAMPLES OF WHAT
THEY'VE DONE.
AND THE MORE SPECIFIC YOU
CAN BE, AND IN YOUR CASE IN
PARTICULAR, I THINK OF YOUS
ALIKE THE BIGGEST TURTLE AT
THE BOTTOM, PERHAPS OR IS IT
THE SMALLEST AT THE TOP.
MAYBE WE COULD HAVE HAD
SOMEONE WHO MINES SILICON
FOR A LIVING AND TALK ABOUT
THAT.
BUT OTHER THAN THAT, RIGHT,
YOU ARE WHERE IT KIND OF
BEGINS, WHAT IS A CHIPSET
MANUFACTURER AND PROCESSOR
MANUFACTURER, WHAT DO THEY
DO TO INSURANCE MOBILE
SECURITY?
>> SO YEAH, ON THIS SLIDE
WHERE IT'S A LITTLE GREEN
BOX AT THE TOP, SOME OF THE

OTHER SLIDES A GRAY BOX AT THE BOTTOM, SO IF YOU THINK ABOUT A MODERN MOBILE DEVICE, THINK ABOUT THE PROCESSOR THAT IS ON IT.
IT'S REALLY NOT A SINGLE PROCESSOR.
IT'S MORE LIKE, YOU KNOW, A SYSTEM OF A DOZEN OR SO PROCESSORS THAT ARE PACKAGED UNDER A SINGLE CHIP.
SO A DOZEN PROCESSORS DO DIFFERENT THINGS.
THEY RUN THE OPERATING SYSTEM, THE APPLICATION, THEY RUN THE BASEMENT SOFTWARE, BLUE TOOTH, A LOT OF THE THINGS STEVE TALKED ABOUT.
BEFORE EVEN THE OPERATING SYSTEM AND APPLICATIONS GET ON THERE, THERE ARE 10 MILLION PLUS LINES OF CODE AND FIRMWARE THEY ARE RIDING ON IT.
THAT IS WHAT WE PROVIDE, THIS FOUNDATIONAL PIECE FOR A LOT OF THESE MOBILE DEVICES.
AND THE JOB OF MY TEAM IS TO MAKE SURE THAT THAT CORE COMPONENT IS SECURE.
THAT WHICH PROPERLY ADDRESSING ITS ATTACK SURFACE THAT IT REPRESENTS THAT ARE ENABLING THE SECURITY FEATURES, THAT THE PARTNERS DOWNSTREAM CAN USE, THE OEMs, CARRIERS, CONTENT PROVIDERS AND DEVELOPERS CAN USE.
BUT ALSO THE PRIMARY FOCUS ON MY TEAM IS MAKING SURE THAT THE SOFTWARE AND HARDWARE THAT WE CONTRIBUTE IS SECURE.

SO STATIC ANALYSIS, DYNAMIC ANALYSIS, MAKE SURE THE MODERN MEASURES ARE ABLED TO --
>> IT'S THE SAME THINGS EVERYBODY IS DOING.
>> JUST TO MAKE CLEAR, I'M SURE THERE IS A LOT OF VARIANCE IN THE ROOM ON WHAT PEOPLE KNOW.
SO WHERE THE CODE AM IN PARTICULAR THAT ARE YOU CONTRIBUTING, ARE YOU DOING THIS AT THE-- HIGHER UP, OFFERING STKs FOR END-USERS, ALL OF THE ABOVE?
>> SO THERE ARE SOME DRIVERS THAT GO INTO THE-- LEVEL, BUT FOR ITS MOST PARDON IT IS-- PART IT IS CODE TO THE LOW THAT OR THE SIDE OF IT.
THAT ARE STILL ON THE SAME SYSTEM.
>> OKAY.
OKAY.
SO THEN JON, I DON'T KNOW IF YOU ITEM ALLLY ALLOWED TO DO THIS, BUT I WOULD LOVE FOR YOU, PROVIDED WE DON'T HAVE ON THE PANEL RIGHT NOW IS SOMEONE WITHOUT WORKS JUST FOR A CARRIER.
A LOT OF YOU, PROMINENT MEMBERS ARE CARRIERS SO SAME SORT OF QUESTION, WHAT DOES THE CARRIER SEE AS ITS ROLE IN THE SECURITY ECOSYSTEM, WHAT DOES IT DO NOT TO, WITH SOMEONE ELSE'S PROBLEM, ET CETERA.
>> SO WILL ME BEGIN BY MAYBE ANSWERING THE QUESTION AT A HIGH LEVEL AND THEN I WILL TRY TO GET INTO THE SPECIFICS.
BUT AT THE END OF THE DAY WHEN YOU LOOK ACROSS THE

ENTIRE MOBILE EQO SYSTEM IT
IS IN EVERYONE'S INTEREST
THAT ALL OF YOU CONTINUE TO
USE YOUR SMART PHONES,
RIGHT.
BECAUSE THAT DRIVES THE
ECOSYSTEM, THAT DRIVES THE
VALUE PROPOSITION.
IT DRIVES THE SIGNIFICANCE
THAT IT HAS FOR EVERY PLAYER
IN THE ECOSYSTEM SO IT IS A
SHARED INTEREST.
A COMMON OBJECTIVE.
ALL OF THE PLAYERS HAVE
DIFFERENT ROLES TO PLAY AND
THAT'S WHY WE HAVE WHAT I
DESCRIBED EARLIER AS THE
CYBERSECURITY WORKING GROUP
WHERE WE ALL GET TOGETHER.
THE CARRIERS ARE THERE.
THE OEMs ARE THERE, THE
PLATFORM PROVIDERS, SO ON
AND SO FORTH.
WHAT WE TRY TO DO IS REALLY
LOOK AT AGAIN WHAT ARE THE
NATURE OF THE THREATS AND
WHAT ARE THE KINDS OF THINGS
WORKING EFFECTIVELY,
COUNTERMEASURES IN THE
MARKETPLACE AND WHAT ARE THE
THREATS WE NEED TO
ANTICIPATE.
NOW EVERY PLAYER INCLUDING
CARRIERS JUST LIKE YOU HEARD
THIS MORNING AND ACROSS A
DIFFERENT PLATFORM PROVIDERS,
CARRIERS HAVE DIFFERENT
MODELS, DIFFERENT SCALES,
THERE IS SMALL, LARGE.
BUT THEY ALL HAVE AS A
PRIORITY SECURITY.
SO THEY ARE ALL TRYING TO DO
EVERYTHING THAT THEY CAN TO
SECURE THE NETWORK, SECURE
THE CAPABLE THEY ARE
DELIVERING TO THEIR

CONSUMERS BUT THERE ARE
THINGS THEY DON'T HAVE
VISIBILITY TO.
SO FOR INSTANCE I WILL GIVE
YOU A CLEAR EXAMPLE AND WE
HIGHLIGHT THIS IN OUR WHITE
PAPERS.
CARRIER MAY HAVE VISIBILITY
TO INFORMATION THAT
TRAVERSES THEIR NETWORK THAT
IS GOING TO BE A MOBILE
DEVICE PARTICULARLY AS IT
RELATES TO INFORMATION THAT
COULD BE THROUGH AN SMS OR
THROUGH OTHER SOURCES.
HOWEVER IF THAT DEVICE IS
TETHERED TO A PC OR TETHERED
TO A I WOULD FEW AND NOW YOU
ARE USING A I WOULD FEW
CONNECTION TO THE INTERNET,
THE CARRIER HAS NO
VISIBILITY TO THAT, NUMBER
ONE.
NUMBER TWO THERE IS NO-- IF
THEY CHOOSE TO JAILBREAK, A
CONSUMER CHOOSES TO DOWNLOAD
INFORMATION FROM A
SUSPICIOUS WEB SITE, IT'S
REALLY UP TO THEM.
SO THERE ARE THOSE ELEMENTS
THAT THE CARRIER DOESN'T
HAVE DISABILITY TO AND IN
SOME SENSE IS SOMETHING THAT
AGAIN THERE IS VERY LITTLE
THAT THEY CAN DO.
BUT AT THE END OF THE DAY
WHEN IT COMES TO THE NETWORK,
THAT'S WHAT THE CARRIER IS
FOCUSED ON IS SECURING THE
NETWORK TO INSURANCE THAT
NOTHING MISCHIEFUOUS OR
MALICIOUS HAPPENS VIS-A-VIS
THE SERVICE.
>> SO YOU COULDN'T HAVE SET
THIS UP BETTER.
I HAVE A QUESTION FROM THE

AUDIENCE.
I REALLY DO WANT TO GET THE AUDIENCE ENGAGED.
A MEMBER OF THE AUDIENCE ASKED THE QUESTION EXACTLY ABOUT THE POINT YOU JUST MADE OR SOMETHING RELATING.
WHICH IS I AM A CUSTOMER OF A CARRIER WHO SOMEONE OF YOUR MEMBERS AND I GOT THE E-MAIL THAT SAID YOU SHOULD TURN ON I WOULD FEW ALL THE TIME, IT WILL HELP YOU WITH YOUR BATTERY LIFE.
IT DIDN'T SAY O AND IT'S ALSO GOING TO PROBABLY HELP US WITH SOME OF OUR ELECTRONIC MANAGEMENT.
BUT THE QUESTION IS HOW DOES THAT OVERLAY THE SECURITY ISSUE.
SO AS THE CARRIERS ARE ARE ENCOURAGING USERS TO USE I WOULD FEW MORE OFTEN OR IN SOME CASES ACTUALLY BUILDING SYSTEMS THAT TAKE ADVANTAGE OF PUBLIC I WOULD FEW.
>> GREAT QUESTION.
I WILL USE MYSELF AS AN EXAMPLE.
JUST BECAUSE I HAPPEN TO BE ON ONE OF THE LARGE FOUR CARRIERS THAT ARE HERE IN THE DC AREA.
THEY LIKE THE COLOR RED BY THE WAY.
BUT WHAT THEY DO OFFER IS THEY HAVE A FOR FREE SECURITY APPLICATION THAT I COULD DOWNLOAD FROM THE CARRIERS STORE THAT WILL MONITOR AND CHECK ON ANYTHING THAT IS ON MY DEVICE.
THAT'S NOT TO SUGGEST THAT IT'S FOOLPROOF BECAUSE THERE

IS NO SYSTEM THAT IS
FOOLPROOF REGARDLESS IF IT
COMES ARE FROM THE CARRIER
OR THE SECURITY COMPANY.
BUT AT THE END OF THE DAY
THOSE THINGS ARE IN PLACE.
AND THE CARRIER IS TAKING
THOSE EXTRA STEPS TO PROVIDE
THOSE CAP ABILITIES TO THE
CONSUMER SO THAT, INDEED,
EVEN IF THEY ARE USING I
WOULD FEW AND SOMETHING
MALICIOUS HAPPENS, OVER THE
I WOULD FEW NETWORK, AT
LEAST THEY HAVE THE RECOURSE,
NUMBER ONE.
SECONDLY, THEY'RE ALSO
PROVIDING ADVICE AND TIPS
THAT IN THE EVENTUALITY THAT
SOMETHING BAD DOES HAPPEN
THIS IS HOW YOU RECOVER.
AND THERE ARE A SERIES OF
TIPS THAT THE-- HAS OFFERED
AND THE INDIVIDUAL CARRIERS
HAVE IT ON THEIR WEB SITES
IN TERMS OF THINGS LIKE IF
YOUR-- GETS INFECTED MAKE
SURE YOU HAVE EVERYTHING
BACKED UP SO YOU CAN RESTORE
IT TO FACT REE SETTING AND
RESTORE THE INFORMATION FROM
YOUR BACKUP OR --
>> BUT AGAIN, MY POINT IS
THAT THE CARRIERS DO
EVERYTHING THEY CAN TO
PROTECT THEIR CUSTOMER.
BUT THERE ARE THINGS THAT
ARE OUTSIDE OUR CONTROL,
NUMBER ONE AND NUMBER TWO NO
SYSTEM IS FOOLPROOF SO YOU
HAVE TO BE PREPARED FOR THE
EVENTUALITY.
>> SO JOHN, YOUR COMPANY AND
CORRECT ME IF I HAVE THIS
WRONG, ARE YOU WITH US
BECAUSE YOU HAVE DONE SO

MUCH KIND OF ANALYZING JUST ABOUT EVERY PIECE OF THE ECOSYSTEM.
SO MAYBE KIND OF IF YOU CAN TAKE THE 25,000 FOOT LEVEL OF THIS MATH AND TALK ABOUT WHERE YOU THINK SECURITY IS HAPPENING AND MAYBE WHERE IT ISN'T HAPPENING.
KIND OF REFLECTIONS.
>> I THINK THAT'S A GOOD WAY TO FRAME IT IT I'M VERY GOOD AT PUTTING ON MY ATTACKER HAT OR MY-- WHICHEVER YOU PREFER.
WHEN I SEE A PICTURE LIKE THIS UP ON THE SLIDE RIGHT NOW I SEE COMPLEXITY.
COMPLEXITY IS THE ARCH-ENEMY OF SECURITY.
SO EACH OF THESE LITTLE BOXES AND I THINK MORE IMPORTANTLY THE LINES BETWEEN THE BOXES, ARE SORT OF IMPLICIT OR EXPLICIT TRUST RELATIONSHIPS.
THEY'RE ALL AREAS WHERE IF I'M AN ATTACKER I'M GOING AFTER EACH OF THESE PARTICIPANTS IN THIS OFFICE SUPPLY CHAIN.
I'M TRYING TO COMPROMISE THESE SMALL INDEPENDENT SOFTWARE HOUSES THAT ARE PROVIDING THE DRIVERS FOR THE CHIPSETS, FOR THE DEVICES THAT YOU ARE USING.
I'M ALSO LOOKING AT IT FROM A PERSPECTIVE OF THE DELAY THAT COMES.
SO IF I DO REPORT A VULNERABILITY TO GOOGLE OR SOME OTHER MOBILE SOFTWARE .ER AND THEY HAVE TO GO THROUGH THIS ECOSYSTEM OR CHAIN OF OPERATORS, WHETHER

IT'S PLATFORM PROVIDER OR
THE OEM, THIRD PARTY
DEVELOPERS, THE CARRIER WHO
IS RESPONSIBLE FOR FINALLY
PUSHING OUT THAT OVER THE
AIR UPDATE, ALL I SEE ARE
ENORMOUS LINKS OF TIME
MEASURED IN MONTHS AND YEARS
WHERE I HAVE THE ABILITY TO
SORT OF-- I COULD DRAW A
DIAGRAM FROM THE ATTACKERS
PERSPECTIVE WHICH IS I HAVE
AN EXPLOIT WHETHER SOMETHING
I DEVELOPED IN HOUSE MYSELF
OR SOMETHING THAT'S BEEN
PUBLISHED PUBLICLY, THERE
ARE SOME RICH JAILBREAK
COMMUNITIES THAT WILL
HAPPILY GIVE AWAY PRIVILEGE
ESCALATION AND OTHER CLIENT
SIDE EXPLOITS FOR FREE IN
ORDER TO SUPPORT THEIR
JAILBREAKING ACTIVITIES.
I LOOK AT THE PATH FROM AN
ATTACKER TO THE END-USER AND
SEE IT'S MUCH SIMPLER AND
THE TIME LINE THAT ATTACKER
REACHING THAT USER IS
PROBABLY MEASURED IN HOURS
OR DAYS WHEREAS THE TIME
LINE FROM A VENNER LIKE
GOOGLE WHO RECEIVES A REPORT
OF VULNERABILITY AND PASSES
IT THROUGH, EVENTUALLY
REACHING THE DEVICE AGAIN IS
MEASURED OUT LIKE A TIME
SCALE AM WHEN ARE YOU
TALKING ABOUT A WINDOW OF
VULNERABILITY IN TERMS OF
SECURITIES, THE ATTACKER IN
MANY CASES IN THAT KIND OF
SEVERAL ORDERS-- THOSE
WINDOWS THE ATTACKER WILL
WIN THAT RACE EVERY TIME.
I CAN TRUST THAT WITH THE
DESK TOP WORLD, WHERE WE

TALKED PREVIOUSLY ON SOME OF THE PANELS ABOUT VERY PROACTIVE COMPANIES LIKE GOOGLE, PUSHING OUT CHROME SECURITY UPDATES IN A MATTER OF HOURS ON THE MOBILE SIDE WE'RE TALKING ABOUT MONTHS AND YEARS.
>> SO LET ME FOLLOW REALLY QUICKLY BECAUSE ONE OF THE THINGS WE KEPT HEARING IN PANEL ONE ESPECIALLY BUT ALSO PANEL 2 WAS THE IMPORTANCE OF SEPARATING THE POSSIBLE AND THE PROBABLE, THE JUST BECAUSE IT CAN BE DONE DOESN'T MEAN IT ISN'T GOING TO BE DONE AND LOOKING AT INCENTIVE MODELS OF ATTACKERS.
I DIDN'T HEAR YOU WEAVING THOSE INTO THE STORY YOU WERE TELLING.
WHAT DO YOU THINK OF THAT APPROACH.
>> I THINK IT IS A REALLY GOOD POINT.
IF WE BRING BACK DAN'S SORT OF KILL CHAIN WHERE WE ARE TALKING ABOUT HOW THEY CREATE THEIR MALWARE, HOW THEY GET ON THE DEVICE, HOW THEY ESCALATE PRIVILEGES AND MONETIZE OR COMPLETE THEIR ATTACK, YOU HAVE TO LOOK AT EACH OF THOSE STAGES AND LOOK AT THE FEASIBILITY OF SOLVING SOME OF THOSE PROBLEMS OR LIKE HOW DO WE EFFECT THE CONVERSION RATES BETWEEN THOSE DIFFERENT STAGES OF THE ATTACKER FUNNEL, IF YOU WILL.
AND I SEE THAT YES THERE'S SEVERAL WAYS YOU CAN GET ON THE DEVICE WHETHER IT'S

MALICIOUS MOBILE APPS THAT
APPARENTLY AFFECT NOBODY OR
EVERYBODY DEPENDING ON WHO
YOU ARE TALKING TO.
THEIR DRIVE BY EXPLOITS THAT
NO ONE THINKS EXIST EXCEPT
FOR A VERY TARGET ADD TACK
AGAINST EXECUTIVES WHERE
THESE ARE STATES ATTACKING
HIGH PROFILE INDIVIDUALS.
I LOOK AT PATCHING PROCESS
AS THE PLACE WHERE WE HAVE
THE MOST MACRO OPTIMIZATION
WHERE WE UNDERSTAND THE
PROBLEMS IN ALL ASPECTS OF
MOBILE SECURITY.
WE KNOW WHAT THEY ARE.
WE HAVE DEALT WITH THEM IN
THE DESKTOP WORLD.
I SEE THE MOST OPTIZATION
AND IMPACT IN THATIZATION,
AND I THINK KIND OF TIES
BACK TO SOME OF JOHN'S
DISCUSSION.
WHERE I DON'T THINK CARRIERS
ARE IN THE SECURITY GAME.
THEY'RE HERE TO PROVIDE
SERVICE.
TO SELL YOU SOME PRETTY
AWESOME VOICE PLANS AND DATA
OVERAGES, IF YOU HAPPEN BE
TO BE IN CANADA LIKE I WAS,
THAT IS NOT THEIR BUSINESS,
I DON'T THINK IT SHOULD BE
THEIR BUSINESS.
I THINK WE HAVE FAIRLY
EFFICIENT MARKETS.
I DON'T KNOW IF THERE IS AN
EFFICIENT MARKET-- I THINK
THE WEALTH OF THE SECURITY
COMPANIES AND DESING TOP
WORLD, EVEN THE MOBILE FOLKS
WHO ARE TRYING TO GET ON
THIS GAME SOMEHOW ARE KIND
HAMSTRUNG BY THE CONTROL
THAT THE CARRIERS ARE

MAINTAINING, THE PLATFORMS.
SO I THINK THERE IS A BIG OPPORTUNITY FOR CARRIERS TO LOOSEN THAT CONTROL, REALLY OPEN UP THE PLATFORM TO THE MARKET SO THIRD PARTIES CAN PROVIDE THE SECURITY SERVICES.
>> I'M A BIG BELIEVER IN THE RIGHT OF REPLY.
>> I'M NOT GOING TO REPLY ON BEHALF OF THE CARRIERS BUT I WILL SAY I THINK IT IS INSANE THAT PATCHING IS EITHER SOLVED OR A PROBLEM WITH A KNOWN SOLUTION IS A VAST OVERSIMPLIFICATION.
I HAVE YET TO MEET A PERSON THAT REALLY UNDERSTANDS.
DEPTH OF THE PATCHING COMPLEX ABILITY IN THE ECOSYSTEM.
>> SO I WILL MAKE A FEW COMMENTS.
AND I WILL SAY THIS ON BEHALF OF THE CARRIERS.
BECAUSE IT'S FAIR TO SAID THAT SFRUR HAS VESTED HUNDREDS OF MILLIONS OF DOLLARS IN SECURITY SOLUTIONS.
AND AGAIN, I THINK THE CARRIERS HAVE PUT THEIR MONEY WHERE THEIR MOUTH IS.
BUT THEY DO IT FOR REASONS THAT ARE IMPORTANT TO THEM BECAUSE IT'S IMPORTANT TO THE CONSUMER, TO THE SUBSCRIBER.
BUT AGAIN, THE ECOSYSTEM HAS GIVEN US THE WEALTH OF DIVERSITY THAT WE HAVE.
BECAUSE THERE WAS A POINT IN TIME WHERE ALL TELEPHONES WERE PAINTED BLACK.
BUT THAT WAS A LONG TIME

AGO.
AND INDEED, THE MARKETPLACE HAS GROWN VERY DRAMATICALLY AND I DONE THINK WE WOULD HAVE SEEN ALL OF THE PLAYERS ON THE PREVIOUS PANLE THAT WE SEE TODAY IF WE WERE STILL IN THE SAME PARADIGM.
AND I DON'T THINK IT'S REASONABLE TO SAY THAT WE'RE GOING TO TURN BACK THE CLOCK TO AN ENVIRONMENT WHERE, YOU KNOW, THERE'S ONE PARTICULAR ENTITY THAT DECIDES HOW SECURITY IS ARCHITECTED IN AN ECOSYSTEM LIKE THIS BECAUSE IT'S THE STRENGTH AND DIVERSITY OF THE ECOSYSTEM THAT MAKES IT VERY HARD TO ATTACK.
AND THE NUMBERS SPEAK FOR THEMSELVES BECAUSE AGAIN, IF YOU HAVE A SINGLE POINT THAT CONTROLS SECURITY, IT'S VERY EASY FOR THE HACKERS AND THE ATTACKERS TO FIGURE OUT HOW TO HAR GET THAT AND MOST MILITARY STRATEGIST WAS EXPLAIN THAT TO YOU.
IN FACT KEITH ALEXANDER, A GOOD PERSON THAT HAS SPOKE PEN ABOUT THAT PARTICULAR, SO THE DIVERSITY OF THE SYSTEM IS ACTUALLY ONE OF ITS STRENGTHS.
THE CARRIERS ARE DOING THEIR PART, ALL OF THE DIFFERENT PLAYERS ARE DOING THEIR PART BECAUSE I SEE THAT EVERY DAY.
AND INDEED THE NUMBERS SPEAK FOR THEMSELVES.
SO TO SAY THAT THERE IS A PROBLEM AND YOU KNOW, A SOLUTION IN SEARCH OF A PROBLEM ISN'T NECESSARILY

WHERE I THINK THE INDUSTRY NEEDS TO BE FOCUSED.
BECAUSE THE RISK OF FOCUSING ON SOMETHING THAT'S NOT THE PROBLEM IS THAT YOU ARE DIVERTING OF RESOURCES FROM WHAT THE INDUSTRY IS DOING TO STAY AHEAD OF THE BAD GUYS AND THAT'S ACTUALLY GOING TO BACKFIRE AND HAVE UNINTENDED CONSEQUENCES.
SO WE CAN'T OVERSIMPLIFY THIS TO A LARGE EXTENT BECAUSE I THINK IT LOSES SIGHT OF WHAT THE REAL ISSUES ARE.
AND THE REAL ISSUES ARE TAKING THE METRICS WE'VE SEEN REPORTED AND IN THE INDUSTRY BASED UPON REAL STATS THAT THEY PULLED FROM WHAT THEY SEE IN THE WILD AND ACTUALLY FOCUSING ON WHAT DO WE NEED TO DO TO KEEP THOSE STATISTICS WHERE THEY ARE OR IMPROVE UPON THEM.
>> SO I DON'T HAVE TWITTER IN FRONT OF ME.
I'M GUESSING PEOPLE ARE SAYING LET'S TALK ABOUT PATCHING FOR THE ENTIRE HOUR.
I'M TO THE GOING TO TAKE THAT BAIT JUST YET BUT I WANT TO COME BACK TO IT IN A BIT.
BUT LET'S FINISH THIS FIRST ROUND AND GET BACK TO THAT TOPPLE-- TOPICS AND OTHERS LATER.
WHEN I WATCHED THAT LAST PANEL IT WAS INTERESTING BECAUSE THEY WERE THE PLATFORMS TALKING BEFERING THEY ARE DOING FOR THE APP

DEVELOPER AND ALSO TO SKRUTS
NIZE ITS ACH DEVELOPER.
I THINK YOU BRING A TOTALLY
DIFFERENT PERSPECTIVE.
ARE YOU THE APP DEVELOPER
NOT ONLY THAT I THINK IS
FAIR TO SAY THAT YOUR
COMPANY ENGAGES PROBABLY AS
A VAST DIVERSITY THAN ALMOST
ANY COMPANY ON EARTH SO WHAT
IS YOUR COMPANY THINK ABOUT
ITS ROLE IN SECURITY.
I MEAN JOHN MARINO JUST SAID
IT'S EVERYBODY'S BUSINESS
AND THAT IS KIND OF THE
MILITARY MODEL.
SO WHAT DOES FACEBOOK THINK
ABOUT ITS ROLE WHEN IT COMES
TO SECURING THE APPS THAT
YOU ARE DESIGNING AND
APPLYING.
>> .
>> FOR ITS ROLE THAT I'M
HERE FOR IS REALLY TO
REPRESENT THE-- APP
DEVELOPER-- I REALLY WANT TO
TRY TO NARROW THE SCOPE HERE
TO THINGS THAT AN APP
DEVELOPER CARES ABOUT ON
MOBILE-- WE COULD FILL UP
SEVERAL PANELS TALKING ABOUT
THE AMOUNT OF TOUGH THAT
GOES INTO THE NORMAL
SECURITY DEVELOP-- AROUND
APPLICATIONS IN GENERAL BUT
NARROWING IT DOWN JUST TO
THE THINGS THAT ARE
DRAMATICALLY DIFFERENT FOR
US ON MOBILE VERSUS THE --
ONE OF THE BIGGEST THINGS
THAT WE STRUGGLE WITH ON AN
APP DEVELOPER IS THE ONE OF
THE PRIMARY SECURITY
MECHANISMS THAT EXIST --
>> THOSE ARE A VERY WELL
UNDERSTOOD PROBLEM ON THE

WEB.
WE DO NOT HAVE A LOT OF
INFORMATION ON-- ON THE WEB,
WE HAVE A LOT OF EXPERIENCE
DEALING WITH ENFORCING-- ON
BROWSERS AND I THINK BOTH
LARGE WEB SITES HAVE-- IN
THE MOBILE SPACE THE SAND
BOXES END UP BEING A LOT
MORE SLIGHTLY DIFFERENT.
WHEREAS WHEN ARE YOU DEALING
WITH FACEBOOK ON A DESKTOP
IT'S VERY COMMON FOR US AS
THE APP DEVELOP TORE KIND OF
SEE CONTROL TO ANY SOFTWARE
RUNNING.
WE'RE REALLY ONLY PROTECTING
FACEBOOK FROM OTHER WEB
SITES, OTHER DOMAINS BUT
IT'S NOT SOMETHING WE
CONSIDER CAN.
IT'S UNFORTUNATE BUT IT'S
NOT A SECURITY OR PRIVACY
VULNERABLE IN FACEBOOK IF
THERE HAPPENS TO BE MALWARE
RUNNING ON A DESKTOP
COMPUTER.
WE SPEND TIME HIT
MYING-- MINIMIZING THAT.
WHEN YOU START APPROACHING
MOBILE DEVICES THERE ARE A
LARGE NUMBER OF WAYS WHERE
SOMETHING FROM FACEBOOK CAN
ESCAPE THE SAND BOX AND
INTRODUCES THE INFORMATION
DISCLOSURE.
THAT'S THE FIRST MAJOR
CATEGORY THAT IS DIFFERENT
FOR US.
ALSO BEING A PLATFORM
DEVELOPER, PLATFORM
DEVELOPER ON A PLATFORM, WE
INTEGRATE WAY LARGE NUMBER
OF APPLICATIONS WITHIN THE
MOBILE-- WHICH MEAN WES ARE
INTENTIONALLY ESCAPING THAT

SAND BOX IN ORDER TO
INTERACT WITH ANOTHER
APPLICATION.
AND SO THE EFFORT THIS WE
END UP FOCUSING ON WHEN IT
COMES TO INFORMATION
DISCLOSURE IS NOT JUST FROM
WITHIN FACEBOOK APPLICATION
BUT FROM WITHIN ALL THE
OTHER APPLICATION SAND BOXES
INTERACTING WITH FACEBOOK,
THE USER HAS CHOSEN TO
EXPORT THE DATA.
AND THE TYPE OF
VULNERABILITIES WE'RE
TALKING ABOUT HERE ARE VERY
UNINTENTIONAL, ALMOST.
THE READ LOGS EXAMPLE THAT
THE PANEL EARLIER TOUCHED ON
IS A GOOD ONE.
SOME APPLICATION LOGGINGS
INTO THE SYSTEM, THE MOST
BASIC TYPE OF PRIVACY
DISCLOSURE YOU HAVE FROM
FACEBOOK IS JUST THE USER T
IS VERY THE KEY IN EVERY-- I
CALL IT IN JUST ABOUT EVERY
PAGE THAT YOU ARE DOING,
ANYTHING SOCIAL AND VERY
EASY FOR ANY DEVELOPER WHO
IS DOING VERY LEGITIMATE
LOGGING OR DEBUGGING, JUST
BASIC EXCHANGE OF
APPLICATIONS TO INCLUDE
THAT.
SO WE HAD MORE READ LOG
INFORMATION WAS THE SOURCE
OF MORE SINGLE IN OUR
ECOSYSTEM THAN ANY OTHERS.
IT'S REALLY GREAT TO SEE
PEOPLE SCALING THEM BACK.
TO CLARIFY IT'S NOT JUST OUR
APPLICATION WRITING INTO THE
APPS, IT'S ANY OTHER
APPLICATION OUT THERE.
>> THOSE ARE THE TYPE OF

PRIVACY VULNERABILITIES THAT
ARE REALLY HARD TO TACKLE AS
AN APPLICATION DEVELOPER AND
YOU END UP DEPENDING ON THE
RELATIONSHIP WITH THE
PLATFORM TO TRY TO HELP
WHILE AT THE SAME TIME
RECOGNIZING THAT THAT TAKES
A LOT OF TIME.
AND SO END UP REALLY TRYING
TO GUIDE OTHER APPLICATIONS
AT THE SAME TIME.
>> THE SECOND PIECE THAT I
WANTED TO TALK ABOUT TO
TOUCH ON THAT IS SLIGHTLY
DIFFERENT FOR US IS THE
SOCIAL ISSUES.
THIS IS KIND OF A BIT
OUTSIDE THE-- ABOUT SECURITY
BUT THERE WAS A COMMON TREND
ACROSS THE PANEL EARLIER
WHERE MOST OF THE ACTIONS
BEING TAKEN BY USERS AS A
RESULT OF SOMETHING THE USER
WANTED.
WE END UP BEING THE SOURCE
OF A NUMBER OF THOSE, THERE
ARE A LOT OF USERS OUT THERE,
A LARGE PERCENTAGE OF OUR
USERS WHO DON'T LIKE THE
COLOR BLUE OR MAYBE THEY
JUST REALLY LIKE THE COLOR
PINK.
SO YOU GO TO JUST ABOUT ANY
OPEN APP STORE AND SEARCH
FOR PINK FACEBOOK YOU WILL
FIND A LARGE NUMBER OF IT
JUST COMPLETE CLONES OF
FACEBOOK-- THE DEVELOPER IS
CREATING THIS PINK FACEBOOK
ARE NOT DOING OUT OF THE
GOODNESS OF THEIR HEARTS AND
THOSE APPLICATIONS COME A
LOT-- ALONG WITH OTHER
SURPRISES.
AND THAT DOESN'T QUITE FIT

THE NORMAL DEFINITION OF MALWARE.
I REALLY LIKE THE GENTLEMAN FROM FAT SKUNK ENCOURAGE US TO REALLY BE CLEAR WHAT WE ARE TALKING ABOUT WHEN WE REFER TO MALWARE.
BUT THAT IS SOMETHING THAT IS NOT TRADITIONALLY REFERRED TO AS MALWARE BUT SOMETHING FACEBOOK WOULD REFER TO AS MALWARE.
I THINK THE SHEER NUMBER OF THINGS THAT COULD POTENTIALLY BE CLASSIFIED AS MALLWARE IS WHAT LEADS TO A LOT OF CONFUSION.
THERE ARE VERY FEW-- THEY DO EXIST.
BUT THERE ARE SEVERAL MILLION USERS WHO WANT FACEBOOK AND HAVE INSTALLED PINK FACEBOOK AND THOSE ADD UP TO REAL --
>> THE TRADEMARK LAWYERS HAVE FOUND THAT AS WELL.
I MEAN A COUPLE OF THE THINGS YOU SAID I WILL STICK WITH YOU FOR A SECOND, KIND OF TALK ABOUT YOUR RELATIONSHIP WITH THE PLATFORM AND TALKED ABOUT WORKING WITH PARTICULAR PLATFORMS SO ONE QUESTION AND I WANT TO KIND OF HEAR OTHER POINTS OF VIEW ON THIS AS WELL, IN THE COMPLEX ECOSYSTEM WHERE WE HAVE ALL OF THESE MOVING PARTS AND AS JOHN SAID, MIND THE ERA, PAY ATTENTION TO THE CONNECTIONS BETWEEN THEM, HOW DOES A MEDIUM BIG COMPANY LIKE FACEBOOK DECIDE WHICH PLATFORMS TO INTERACT WITH, WHAT THE TERMS OF THOSE

RELATIONSHIPS SHOULD BE,
HELPED IN THE LAST PANEL OF
HAVING A VISUAL ARRAY, IS
THAT 9 CRITICAL FACTOR OR
DOES A COMPANY LIKE FACEBOOK
SAY WE'RE GOING TO BE
EVERYWHERE ALL THE TIME AND
DOT BEST WE CAN DEPENDING ON
THE PLATFORM.
>> WE GO TO WHEREVER OUR
CUSTOMERS ARE.
WE TEND TO GET MUCH MORE
HANDS ON, IT APPROACHES A
POINT WHERE A FAIRLY LARGE
PERCENTAGE-- SO WE WRITE OUR
OWN IOS ANDROID APPLICATIONS
WHEREAS ON THE SLIGHTLY
SMALLER PLATFORMS WE WORK
CLOSELY WITH THOSE
PLATFORM-- PLATFORMS
DIRECTLY TO BUILD THEIR OWN
PLATFORMS.
THERE'S VERY TIGHT-- WITH
FACEBOOK OF THE MAJORITY OF
THE CODE WRITTEN ON
MICROSOFT.
SO IT IS A VERY SHARED
RELATIONSHIP.
>> IS THAT A PIECE OF YOUR
DECISION MAKE BEING HOW YOU
WILL IMPLEMENT SOMETHING,
WHETHER YOU GO-- THE
PREFERENCE IS WHICH ONE IS
EASIER TO PERHAPS-- THE
COMPANY AS A WHOLE.
>> SO SAME QUESTION AS THE
OTHER MEMBERS OF DIFFERENT
PARTS OF THE ECOSYSTEM WHICH
IS YOU WANT TO CREATE A NEW
DEAL WITH APPLE OR WITH
BLACKBERRY OR WITH ONE OF
THE MANY ANDROID HANDSET
PROVIDERS.
HOW DO YOU DECIDE WHICH TO
USE, WHICH TO CHOOSE.
AND SPECIFICALLY WHERE TO

SECURITY FACTOR INTO THAT.
IS SECURITY A DOMINANT PART
OF THAT PRO AND CON LIST OR
IS IT, YOU KNOW, MORE
ECONOMICS THAN CONSUMERS AND
EYEBALLS, SO FOR QUALCOMM
WITH HANDSETS, FOR CARRIERS,
YOU KNOW, DECIDING WHICH TO
CARRY, DEPENDING ON THE
OPERATING SYSTEM.
WHERE DOES SECURITY COME TO
THAT DECISION IF AT ALL.
IT'S JUST JUMP BALL, WHOEVER
WANTS TO TAKE THAT.
>> I WILL START.
AND AGAIN ON BEHALF OF THE
ASSOCIATION WHICH IS NOT
JUST THE CARRIERS, JUST TO
CLARIFY.
BUT INDEED, IT'S AS I
MENTIONED EARLIER T THERE
ARE STANDARDS AND PRACTICES
THAT ARE ASSOCIATED WITH
SECURITY.
JUST THE WAY THAT THERE ARE
STANDARDS AND PRACTICES
ASSOCIATED WITH THE
TECHNOLOGY.
WE HEARD SOME OF THE
SPEAKERS EARLIER TALK ABOUT
THAT.
SECURITY IS ALWAYS PART OF
THE DISCUSSION.
PARTICULARLY GIVEN NOW THAT
THERE IS AN EXECUTIVE ORDER
IN FEBRUARY OF THIS YEAR, BY
THE PRESIDENT.
AND IN FACT THAT'S BEEN A
RALLYING POINT ACROSS 16
DIFFERENT SECTORS AND
WORKING WITH THE GOVERNMENT
AND ON ITS EXECUTIVE BORDER
AND IN DELIVERING THE
NATIONAL SIDE OF THE
SECURITY FRAMEWORK IN RECORD
TIME BECAUSE THE FIRST DRAFT

IS SUPPOSED TO BE DONE BY
OCTOBER.
I WAS IN PITTSBURGH LAST
WEEK, BY THE WAY, THERE WERE
400 PEOPLE THAT SHOWED UP
FOR THAT SECOND WORKSHOP WAS
MISSED SO INDEED THE
INDUSTRY IS FOCUSED.
AND I WOULD CITE THAT AS
EXAMPLES BE HOW IMPORTANT
CYBERSECURITY IS
ACROSS-THE-BOARD.
AND IF EVERYTHING GOES
ACCORDING TO PLAN, THE
CYBERSKOOURT FRAMEWORK WILL
BE DONE BY FEBRUARY OF NEXT
YEAR.
AS REQUIRED BY THE EXECUTIVE
ORDER.
AND INDEED, ALL OF THE
PLAYERS ARE AT THE TABLE
INCLUDING THE MOBILE
INDUSTRY.
SO FROM THAT PERSPECTIVE, I
THINK, AGAIN, THAT IS A
CLEAR FOCUS AND A CLEAR
PRIORITY ON BEHALF OF THE
NATION RELATIVE TO HOW THIS
IS IMPORTANT TO THE ENTIRE
ECOSYSTEM ACROSS 16
DIFFERENT SECTORS.
BECAUSE THE THREATS ARE
REAL.
WE DON'T DISMISS AT ALL ANY
OF THE THREATS AND THE
INVESTIGATORS THAT WE'RE
SEEING AND THE STATISTICS
THAT ARE OFTEN TALKED ABOUT
IN THE PRESS.
THE REALITY IS IT'S COMPLEX.
THE REALITY IS, IS THAT
THERE IS NO, YOU KNOW, EASY
FIX BECAUSE AGAIN WE LIVE IN
A VERY DYNAMIC AND OPEN
MARKETPLACE.
AND WE HAVE TO RESPECT THAT.

BUT ALSO THEN KEEP IN THE CONTEXT OF HOW DO WE DELIVER SECURITY.
AND THAT IS A TOP PRIORITY.
>> I THINK IF I COULD TAKE OFF MY ATTACKER HAT FOR A LITTLE BIT AND PUT BACK ON MY APPLICATION DEVELOPER AS A TWO FACTOR AWE THEN CASE COMPANY THAT OFFERS AUTHENTICATION SERVICES ON PRETTY MUCH EVERY MOBILE PLATFORM OUT THERE, I DO HAVE TO AGREE WITH ALEX THAT MOST BUSINESSES ARE GOING TO FOLLOW WHERE THEIR USERS ARE.
THEY'RE GOING TO FOLLOW THAT DEMAND.
YES, SECURITY ESPECIALLY A TWO FACTOR SERVICE IS ABSOLUTELY PARAMOUNT.
BUT WE ALLOW THE CUSTOMERS TO MAKE DECISIONS ABOUT WHAT PLATFORMS THEY WANT TO SUPPORT.
IF SAY YOU HAVE A CORPORATE POLICY THAT SAYS YOU CAN ONLY USE THIS APPLICATION ON THE LATEST VERSION OF ANDROID THAT'S FULLY PATCHED, WE CAN DESIGN-- DEFINE IT SO GIVING USERS SOME CONTROL OR EVEN ENTERPRISE SOME CONTROL WHILE STILL COVERING ALL OF YOUR BASIS, ESPECIALLY FOR CONSUMER SERVICES, THAT IF YOU DECIDE NOT TO SPORT A PLATFORM, THOSE USERS SIMPLY ARE GOING TO USE YOUR SERVICE.
I THINK THAT'S GOING TO BE COMMON ACROSS MOST APPLICATION PROVIDERS.
THEY PROBABLY DON'T SEE SECURITY AS THEIR TOP

CONCERN.
THEY'RE LOOKING AT ADOPTION RATES, OR JUST THE USEABILITY.
>> GO AHEAD.
>> TO FOLLOW ON THAT, INDEED, YOU KNOW, YOU DO HAVE TO FOLLOW THE CUSTOMER.
BUT INDEED, YOU DO THAT BY MAKING SURE YOU HAVE A VARIETY OF SOLUTIONS THAT ADDRESSES THEIR NEEDS AND REQUIREMENTS.
AND TO YOUR POINT ABOUT THE ENTERPRISE, ARE YOU ABSOLUTELY RIGHT AND THAT'S WHY ENTERPRISES ARE NOW EMPLOYING THINGS LIKE MOBILE DEVICE MANAGEMENT PLATFORMS THAT HELP MANAGE POLICY ASSOCIATED WITH SECURITY FOR THOSE DEVICES THAT ARE USED INSIDE THE ENTERPRISE, PARTICULARLY IN AN ENVIRONMENT WHERE INCREASINGLY YOU HAVE BRING YOUR OWN DEVICE INTO THE ENVIRONMENT FOR ACCESS TO PRY PRIOR TEAR INFORMATION, E-MAIL OTHER OTHER APPLICATIONS, SO AGAIN, WE DO HAVE TO AS AN INDUSTRY KEEP IT EASY AN SIMPLE FOR THE APP DEVELOPERS BECAUSE WE WANTED TO CONTINUE TO FLOURISH IN TERMS OF THE APP ECONOMY.
AND THAT'S REALLIED CHALLENGE.
BECAUSE WHEN YOU BUILD A HOUSE YOU HAVE TO BUILD SECURITY INTO EVERY ELEMENT IN THE HOUSE FROM THE FOUNDATION TO THE LOCKS ON THE DOORS, THE LOCKS ON THE WINDOWS, ALL ITS WAY UP

THROUGH YOU, KNOW, EVERYTHING THAT YOU ARE DOING TO MAKE SURE IT PROVIDES A SAFE AND SECURE ENVIRONMENT.
AND PERHAPS NOT A PERFECT ANALOGY BUT IT IS GOOD WHEN YOU LOOK AT CYBERSECURITY ACROSS WHAT IS A VERY COMPLEX ENVIRONMENT.
BUT AT THE END OF THE DAY WE ARE KEEPING IN MIND ALL OF THOSE REQUIREMENTS BECAUSE WE HAVE TO FOLLOW --
>> SO LET ME, THE ONE THING WE DON'T HAVE ON THIS PANEL IS CLOSEST, IS WE DON'T HAVE THE TINY APP.
YOU DON'T HAVE THE PROVERBIAL TWO PEOPLE IN THE GARAGE WHO ARE BARELY, BARELY FOCUSING ON THEIR FEATURES.
AND THE LAST THING THEY NEED TO BE TOLD IS SECURITY SERVICES, PRIVACY IS THEIR BUSINESS, LEGAL COMPLIANCE IS THEIR BUSINESS.
WE OFTEN HEAR THAT THIS IS TIED TO THE KIND OF HELP OF THE INNOVATION ECONOMY AS WELL.
IT'S A GOOD THING THAT MAYBE THEY CAN FOREFALL PART OF THAT ATTENTION.
JOHN, YOU'RE A COMPANY THAT PROBABLY THINKS A LOT ABOUT SECURITY SINCE ARE YOU TRYING TO SELL A SECURITY RELATED PRODUCT SO WHAT SHOULD WE TELL THOSE SMALL TWO PEOPLE DEVELOPERS AND THEIR FIRST TWO MONTHS, THEY'RE GETTING READY TO DROP OUT OF HARVARD BECAUSE THEY SAW THE MOVIE AND THIS

IS A WAY TO MAKE A LOT OF
MONEY.
IS SECURITY THEIR BUSINESS.
IS IT TRUE THAT LITERALLY
EVERY MEMBER OF THE BUILDING
OF THE HOUSE, IS THAT THE
METAPHOR YOU JUST USED, HAS
TO THINK ABOUT SECURITY OR
DO SOME OF THEM GET A PASS
AN OTHER PEOPLE JUST HAVE TO
HELP THEM.
>> I THINK THAT'S THE DANGER
WITH, I MEAN BROADER THAN
MOBILE.
MOBILE ADOPTION
AND-- COMPUTING IT MAKES IT
REALLY EASY TO SCALE SERVICE
AND TO BUILD AN APPLICATION
WHERE YOU GET TWO GUYS IN A
GARAGE, YOU CAN DEVELOP AN
APPLICATION, YOU CAN SCALE
OUT THE LASTING CLOUD
SERVICES TO TENS OF MILLIONS,
HUNDREDS OF MILLIONS OF
USERS, WITH BASICALLY NO
OVERSITE.
SO IF YOU REWIND IT BACK TEN
YEARS AGO, IF YOU HAD AN
APPLICATION THAT WAS
REACHING A HUNDRED MILLION
USERS AND YOU WERE
PROTECTING ALL THEIR DATA,
YOU WOULD HAVE FIKD PIN FROM
STRUCTURE, DATA SERVICES,
SECURITY TEAMS, A VERY
MATURE ENVIRONMENT WHERE NOW
A-DAYS, THE FACT THAT YOU
CAN REACH THESE
OMGATION-- POPULATIONS T IS
KIND EVER A BLESSING AND A
CURES.
YOU HAVE THE ABILITY TO
SCALE A SIMPLE APPLICATION
AND SAY INSTA GRAM TO A
LARGE NUMBER OF USERS
WITHOUT THE TYPICAL

EVOLUTION OF SECURITY
PRACTICES THAT WE USED TO
HAVE IN PLACE IS SO SUDDENLY
ARE YOU IN CHARGE OF ALL
THIS VERY IMPORTANT DATA AND
PRIVACY CONTROLS AND ISSUES.
AND YET YOU HAVE KIND OF
SKIPPED A LOT OF SORT OF
LESSONS IN SECURITY ALONG
THE PATH.
>> I THINK IT HELPS CHANNEL
A LOT OF THE SMALL APP
DEVELOPERS THAT WE WORKED
WITH SINCE WE DO FIND
OURSELVES IN A POSITION OF
PROVIDING-- IT IS KIND OF A
MIXED BAG.
JOHN REALLY HIT ON THE CORE.
PART OF IT IS THE APP DOES
STUFF.
AND YOU DON'T HAVE IT-- AT
THE SAME TIME, THERE IS A
LARGE NUMBER OF SHARED
COMPONENTS BETWEEN THESE.
THEY ARE ABLE TO REACH THE
SCALEDOWN BECAUSE THEY ARE
DEPENDENT ON SO MANY-- AND
BY PLATFORMS I DON'T MEAN
THE PLATFORMS TALKING ABOUT
EARLIER, I'M TALKING ABOUT
FACEBOOK, SOCIAL PLATFORM,
AMAZON INFRASTRUCTURE,
GOOGLE, ANDROID PLATFORM.
ALL OF THOSE PLATFORMS
INVEST HEAVILY IN PROVIDING
DEVELOPERS WITH SOUND,
ADVICE AN GUIDANCE ON HOW TO
USE THEIR PLATFORMS.
SO THE MAIN ADVICE THAT WE
GIVE TO DEVELOPERS TO BUILD
SECURITY IS TO FOLLOW OUR
ADVICE.
AND THE ADVICE OF THE OTHER
PLATFORMS.
THEY REALLY CAN'T BE
EXPECTED TO HAVE SECURE OR

MATURE SECURITY TEAMS THAT
HANDLE ALL OF THESE.
FORTUNATELY THEY ARE
BUILDING ON PLATFORMS THAT
DO HAVE MATURE SECURITY
TEAMS AND ADVICE.
>> BUT YOU BELIEVE THAT YOU
CAN HAVE A LOT OF SECURITY
IN A BOX, BASICALLY.
LIKE YOU GUYS BUILD A SECURE
PLATFORM, YOU HAVE SOME
PROBABLY EASY TO DIGEST
DOCUMENTATION, USER
EDUCATION ABOUT HOW TO BUILD
A SECURE APP.
YOU THINK THAT WILL GET MOST
OF THE WAY OR A LARGE PART
OF THE WAY.
I IMAGINE A PERSON THAT
NEVER HAD A FORMAL SOURCE
COURSE IN SECURITY, NEVER
DID MUCH READING ARE THEY
STILL --
>> YES, NARROWING THE COPE A
GREAT DEAL THERE TO JUST
TALK ABOUT-- IF YOU ARE
FOLLOWING THE FACEBOOK STK
GUIDELINES, WILL YOU END UP
IN A VERY SECURE PLACE WITH
REGARDS TO KNOWN
VULNERABILITIES.
>> HOW MANY HOURS WOULD THAT
TAKE TO READ IT ALL.
I'M JUST CURIOUS, OR THE
SECURITY --
>> THE SECURITY RELATED
STUFF IS QUITE
STRAIGHTFORWARD.
ESPECIALLY FOR-- SORRY, I
DON'T MEAN TO DODGE THE
QUESTION BUT THERE IS A WIDE
RANGE OF-- THE AMOUNT OF
THOUGHT WOULD YOU HAVE TO
PUT INTO SECURITY IS VERY
DIFFERENT DEPENDING ON WHICH
ONE.

THE LOG IN IS THE ONE WHERE
THE SECURITY-- IS MOST
MATURE BECAUSE-- IT IS
NOT-- IT'S TIED RIGHT INTO
THE WHOLE-- IT'S NOT A
SEPARATE THING.
-- WE TRY TO MAKE SURE THE
ONBOARDING PROCESS IS VERY-- IF
YOU SEARCH THROUGH OUR
FACEBOOK DEVELOPER
DOCUMENTATION, WE DON'T HAVE
A LARGE NUMBER OF SECTIONS
THAT ARE CLEARLY TITLED
SECURITY AND SECURITY BEST
PRACTISE.
IF IS LITTERED THROUGHOUT
OUR DOCUMENTATION, WHICH IS
COMMON ACROSS THOSE
PLATFORMS.
EVEN IF YOU TAKE SOMETHING
LIKE ANDROID, THEIR
DOCUMENTATION FOR BUILDING
THE RIGHT WAY IS THEIR
DOCUMENTATION,-- I DON'T
MEAN TO OVEROR
UNDERSTATEMENT THE ISSUE BUT
THAT TENDS TO BE-- I THINK
MOST OF THEM THE PLATFORMS
THAT THEY REPRESENT
DISCUSSED ON THE PANEL HERE
TODAY DO GO OUT OF THEIR WAY
TO MAKE SOME HELP DEVELOPERS
BUILD SECURELY.
>> SO THIS MIGHT BE THE SAME
QUESTION, AND SO JUST TELL
ME, LET'S MOVE ON TO
SOMETHING DIFFERENT.
STEVE IN HIS TALK BROUGHT UP
THE PROBLEM OF THE THIRD
PARTY STKs, PROBLEM MAY BE
THE WRONG WORD TO DESCRIBE
IT, BUT YOU KNOW, GIVING A
TON OF FUNCTIONALITY TO
SOMEONE IN A VERY EASY TO
USE FORMAT.
I NOTE THAT QUALCOMM

ACTUALLY DOES SOME OF THIS
AS WELL.
AND SO THE QUESTION IS HOW
MUCH OF A PART OF THE
SECURITY PROBLEM IS THAT?
RIGHT?
AND WE'RE TALKING I'M SURE
ABOUT DIFFERENT MODELS THAT
HAVE LOOSELY ORGANIZED
SOURCE MODELS AND PROBABLY
EXIST FOR A COUPLE OF MONTHS
AND PEOPLE GOING TO OTHER
THINGS AND YOU HAVE COMPANY
BACKED ONES THAT ARE REALLY
SECURE.
SO IN THE CASE OF THIS, THE
CASE YOU ARE PUSHING AT S IT
LIKE WHAT ALEX RICE WAS JUST
SAYING ABOUT-FACEBOOK, THAT
YOU KNOW, USE IT CORRECTLY,
FOLLOW OUR DOCUMENTATION AND
WILL YOU BE --
>> I THINK OUR CASE IS
PERHAPS MORE COMPLEX.
IT'S NOT THAT WE RELEASE
STKs, BUSINESS-TO-BUSINESS,
SO WE, WHAT WE RELEASE A LOT
OF CASES.
THAT INTEGRATE WITH OR
MODIFY AND THE REASON FOR
THAT IS TO FACILITATE
GREATER INNOVATION,
CUSTOMIZATION AND ENABLE THE
AUDIENCE TO PROVIDE BETTER
PRODUCTS.
NOW WITH THAT COMES THE
CHALLENGE IN TERMS OF
ADDRESSING ISSUES LIKE
ADDRESSING MOBILITIES SO
WHEN WE FIND A VULNERABILITY,
WE HAVE TO WORK WITH THE
OEMs TO GET THOSE ADDRESSED.
SO IS IT'S-- I WOULDN'T CALL
IT A PROBLEM BUT IT
CERTAINLY IS A DUAL EDGE
SWORD.

HELP DRIVE A LOT OF
INNOVATION THAT PRESENTS
SECURITY CHALLENGES.
>> OKAY SO, BEFORE WE MOVE
OFF THAT KIND OF DEVELOPMENT,
ONE MORE QUESTION I JUST,
THIS WASN'T IN MY-- I HAVE
BEEN THINKING ABOUT THIS ALL
DAME I ANY ONE COULD HAVE
WATCHED EVERYTHING UP TO NOW
AND WILL YOU CONCLUDE TWO
THINGS WHICH IS JAILBREAKING
IS ALWAYS BAD.
AND THERE'S NO SUCH THING AS
A RELIABLE, TRUSTWORTHY
THIRD PARTY APP STORE.
AND I JUST WANT TO THROW
THOSE PROPOSITIONS OUT THERE
BECAUSE I PERSONALLY DON'T
BELIEVE THOSE BUT I WANT TO
SEE IF THAT IS WHAT PEOPLE
SHOULD WALK AWAY WITH.
JUMP BALL, DOES ANYONE WANT
TO RUSH TO THE DEFENSE OF
THESE TWO THINGS.
>> WHAT IS JAILBREAKING IS
BAD MEAN.
>> THAT THERE IS NO-- WHEN
THERE IS NO REASON ANYONE
SHOULD DONING IT, LET'S DOT
STRONGEST VERSION, THESE ARE
NOT THE OFFICIAL VIEWS,
STAFF OR COMMISSIONERS.
IS THAT THE-- IS THAT A
MESSAGE WE SHOULD TAKE FROM
THIS?
THAT IF THERE IS SOMEONE OUT
THERE TRYING TO HELP PEOPLE
JAILBREAK PHONES, THEY'RE
PROBABLY DOING A BAD THING
OR IS THIS TYPICALLY --
>> IT'S BEEN A VERY --
>> I HAVE INSTALLED MY OWN
OPERATING SYSTEMS ON MOST OF
MY PHONES, SO THIS IS A VERY
PERSONAL QUESTION FOR ME BUT

I'M ALSO JUST WONDERING.
>> I WILL PUT A VERY CONSUMER HAT ON FOR A MOMENT AND SAY THAT THE CONSUMERS WHO JAILBREAK THEIR DEVICES SO THEY DON'T PAY A $60 TETHERING FEE ARE NOT BAD OR EVIL.
THEY, THAT IS VERY-- IT IS HARD TO CONDONE THOSE PEOPLE AND JUST ACCEPT THAT THEY ARE GOING TO BE-- AND INSECURE BECAUSE THEY WERE TRYING TO OPERATE OUTSIDE THE --
>> IT'S DEFINITELY SOMETHING THAT WE CAN LEAN HEAVILY AGAINST, BUT I THINK WE WOULD BE REMISS --
>> WHAT ABOUT THIRD PARTY, CORRECT ME IF I'M WRONG.
I THINK FACEBOOK HAS SOMETIMES OFFERED SOME OF YOUR APPS.
>> WE DO.
SO THIRD PARTY APP STORE SAY GENERIC TERM TO GIVE YOU AN EXAMPLE AV A GOOD APP STORE, AMAZON, I DON'T WANT TO SPEAK FOR GOOGLE BUT I THINK THAT IS WHAT THEY ARE GOING FOR WHEN-- I THINK THE AMAZON APP STORE SAY VERY GOOD THING.
AND IT IS THIRD PARTY APP STORE.
>> THAT SAID, THERE ARE PROBABLY MORE BAD THIRD PARTY APP STORES THAN THERE ARE AMAZON EXAMPLES.
I WON'T EXTEND IT FURTHER THAN THAT.
IT'S ABSOLUTELY GOOD BECAUSE IT ENABLES THINGS LIKE AMAZON --
>> IT'S JUST ONE COMMENT I

COULD MAKE, ON THE THIRD
PARTY APP STORES.
THE REALITY IS THAT THE
INTERNET HAS NO GEOGRAPHIC-- AND
THE ISSUE IS OFTENTIMES YOU
DON'T KNOW WHETHER, YOU KNOW,
THE APP STORE THAT YOU ARE
ACCESSING, WHETHER
IT'S-- SOMEWHERE IN RUSSIA
OR WHETHER IT'S FACEBOOK
WITHIN THE CONFINES OF THE
UNITED STATES.
SO IT'S THAT COMPLEXITY AND
OPENNESS OF THE INTERNET
THAT REPRESENTS A CHALLENGE
PARTICULARLY WHEN IT COMES
TO APP STORES BUT ONE OF THE
THINGS THAT THE MOBILE
INDUSTRY HAS STARTED TO DO
AND YOU SEE THAT THROUGH THE
EFFORTS OF SOME OF THE
CARRIERS IS THAT THEY WILL
ACTUALLY PROVIDE, NOT
DICTATE BUT PROVIDE
RECOMMENDATIONS TO CONSUMERS
IN TERMS OF APPLICATIONS AND
OR APP STORES, THAT THEY
WOULD RECOMMEND IN THE SENSE
OF PUTTING THEIR BRAND,
BECAUSE AGAIN YOU'VE GOT TO
PROMOTE THE GROWTH OF THE
INDUSTRY AND A LOT OF THAT
IS THROUGH APP STORES.
SO AT THE END OF THE DAY
IT'S A JUGGLING ACT BUT WE
HAVE TO RECOGNIZE THE
REALITY THAT DIFFERENT
DIFFERENT.
>> I WOULD SAY THAT FROM A
PERSPECTIVE OF-- I GUESS
WOULD WOULD SAY IT IS NOT
GOOD FOR SECURITY BUT THERE
ARE CERTAIN CASES WHERE
THIRD PARTY-- ARE GETTING
SECURITY FIXES OUT FASTER
THAN THE OFFICIAL PLATFORM

PROVIDERS, SO YOU TAKE AN EXAMPLE OF A PUBLIC JAILBREAK-- THAT HAS DROPPED THE INTERNET AND YOU THINK ABOUT THE LONG PROCESS IT TAKES FOR PLATFORM PROVIDERS AND OEMs AND CARRIERS TO GET THAT OUT TO USERS.
SOME OF THE THIRD PARTIES HAVE TO GO THROUGH SEC CERTIFICATION AND ALL THESE OTHER REGULATIONS.
THEY CAN PUSH OUT THESE SECURITY PATCHES MUCH MORE AGGRESSIVELY.
OBVIOUSLY THIS IS AT THE EXPENSE OF POTENTIAL STABILITY OF THE DEVICE BUT THERE CAN BE CASES WHERE USING A THIRD PARTY ROM DOES MAKE YOUR DEVICE MORE SECURITY.
SO LET'S AT THE VERY END I WILL GIVE YOU EACH ONE LAST MOMENT TO KIND OF REFLECT BUT LET ME ASK A QUESTION ABOUT PATCHING.
BEFORE WE GET TO THAT MOMENT.
AND I WON'T CALL ON ANYONE BUT THIS WILL BE A JUMP AND I WILL GIVE YOU MY LAW PROFESSOR EVIL EYE IF NO ONE IS ANSWERINGMENT BUT THE WAY I WANT TO KIND OF FRAME IT IS MAYBE PUT A SLIGHTLY MORE POSITIVE SPIN ON IT WHICH IS ASSUME THAT, ASSUME THAT YOU WANT TO INCREASE THE SIGNED OF FREQUENCY, RELIABILITY, SPEED WITH WHICH PATCHES ARE PUSHED ON TO TELEPHONES.
THE STORY THAT I'VE BEEN TOLD IS THAT PART OF THE PROBLEM IS THERE IS A HUGE COORDINATION PROBLEM AMONG

DIFFERENT PEOPLE ON THAT
CHART.
IS THERE ONE QUICK FIX WE
COULD DO TO KIND OF LESSEN
COORDINATION COSTS, TO
RAISIN SEN DIFFICULTS, TO
CHANGE TECHNOLOGICAL
BARRIERS?
LIKE WHAT IS THE NATURE OF
THE PROBLEM, ASSUMING IT IS
A PROBLEM, AND IF YOU WHAT
YOU WANT TO SAY IS IT IS NOT
A PROBLEM, PLEASE FEEL FREE
TO SAY THAT AS WELL.
HOW DO WE MAKE PATCHING
HAPPEN MORE QUICKLY.
>> THAT WAS A LOT OF
QUESTIONS IN ONE.
>> YES, THANK YOU, YOU
NOTICED THAT.
BUT THAT MEANS YOU CAN SAY
ANYTHING AND YOU WILL STILL
BE ANSWERING A QUESTION.
>> THAT QUESTION WAS VERY-- YES,
SO I THINK YOUR ASSUMPTION
IS VALID, RIGHT.
SO I THINK WE DO WANT TO
MAKE IT SIMPLER TO PATCH,
RIGHT.
BUT I THINK OUR MOTIVATIONS
ARE NOT NECESSARILY IN LINE
WITH WHAT JOHN IS SAYING
THERE IS NOT NECESSARILY AN
URGENT THREAT THAT WE'RE
TRYING TO PROTECT AGAINST AM
BUT IN GENERAL IN TERMS OF
PREPARING FOR WHAT THE
FUTURE MAY BRING, WE WANT TO
HAVE -- WE WANT TO FOCUS ON
CONTAINMENT AND BEING ABLE
TO RESPOND.
IT IS A CHALLENGE.
AND SORRY THERE WAS ANOTHER
PART OF THE QUESTION WHICH
IS --
>> SO HELP ME FIGURE OUT HOW

WE BEGIN TO SIMPLIFY.
>> SO BASICALLY, YES.
>> WE'RE NOT SITTING IN THE EASY SOLUTION AND NOT USING IT, I THINK THAT WAS ANOTHER PART OF THE QUESTION, I THERE IS NO EASY SOLUTION THAT WE'RE JUST KEEPING FOR FUTURE USE.
IT'S A REAL CHALLENGE.
WITH MANY STAKEHOLDERS, WITH DIVERGING INTERESTS.
THAT IS ONE OF THE CHALLENGES, RIGHT.
WITH A PC YOU OWN THAT PC.
ARE YOU THE STAKEHOLDER, IT'S YOURS.
FOR LARGER ENTERPRISES IT IS A COMPANY-- IT THERE IS NO QUESTION WITH THE PHONE BECOME A MUCH MORE INTIMATE DEVICE EVEN IF YOU HAVE A COMPANY ISSUED PHONE, YOU HAVE A LOT OF STAKEHOLDERS.
THE ENTERPRISE WHO WANTS TO CONTROL T THE USER THAT WANTS TO CONTROL T THE CARRIER F IT IS SUBSIDIZED, THE ILLUSION THAT THEY STILL HAVE A STAKE IN IT, THE CONTENT PROVIDERS, THE APP DEVELOPERS, THE PLATFORM VENDORS AND WE HAVE THIS, IT'S A REAL CHALLENGE OF MULTIPLE MASTERS, AND FIGURING OUT HOW TO ENABLE THE SYSTEM WHERE YOU HAVE, YOU DON'T HAVE A SINGLE MODE OF TRUST.
WE HAVE THIS REALLY INTERCONNECTED SYSTEM WITH MUTUALLY DISTRUSTED ROOTS.
SO I KNOW YOU STUDIED THE PATCHING EMPIRICS OF IT, DO YOU HAVE A TOP LINE STATISTIC YOU WANT TO SHARE.

>> ONE OF THE THINGS THAT I MENTIONED EARLIER IS WE HAVE KIND OF BEEN DISCUSSING. WHAT IS THE RIGHT MOTIVATION, IF IT IS 2% F IT IS 2-- 001%.
I THINK THAT IF YOU LOOK AT THE PATCHING PROBLEM IN ITSELF, SO WE DID A LITTLE RESEARCH FUNDED BY-- THAT KIND OF LOOKED BROADLY AT THE ANDROIDING SYSTEM.
AND ANDROID IS NOT UNIQUE IN THE WAY ITS PATCHES ARE DISTRIBUTED THROUGH THESE CHAINS OF DIFFERENT RESPONSIBILITIES, OR MUTUAL DISTRUST.
BUT YOU COULD CONTRAST THAT WITH A MODEL LIKE APPLE WHERE ALL THE UPDATES ARE ESSENTIALLY DELIVERED, THERE IS ONLY A HANDFUL OF UNIQUE HAND WARE HANDSETS YOU HAVE TO ATTEST AND CONFIGURE IN, YOU CAN SEE THE ANDROID IS A VERY DIFFICULT ECOSYSTEM TO SECURE AND DELIVER TIMELY PATCHES, SO PART OF THIS RESEARCH IS TO RELEASE THIS APPLICATION CALLED X-RAY WHICH WILL ACTUALLY PERFORM VULNERABILITY ASSESSMENT ON YOUR DEVICE, SO LOOK FOR THE PRESENCE OF VULNERABILITIES, NOT BASED ON THE VERSION NUMBER OR ANY SORT OF MAGIC IDENTIFIERS BUT BY ACTUALLY ANALYZING THE SOFTWARE, THE MACHINE CODE ON YOUR DEVICE.
AND ABOUT 8 MONTHS AGO WE FOUND THAT ABOUT 60% OF ANDROID DEVICES OUT THERE HAVE UNPATCHED INSTALLATION ABILITIES WHICH ALLOW AN ATTACKER TO EITHER-- ESCALATE

PRIVILEGES TO TAKE FULL
CONTROL OF THE DEVICE.
SO WHETHER IT'S .001% OR 2%,
I KNOW SEVERAL PEOPLE IN THE
AUDIENCE TODAY COULD RELEASE
AN-- TOMORROW THAT LEVERAGES
THE PAYLOADS AND KPRI MICE
THE DEVICE, SO WHETHER OR
NOT THE PROBLEM IS HAPPENING
TODAY OR TO HAVE THAT
EXPERTISE, I THINK THAT THE
DELTA BETWEEN WHERE WE ARE
NOW AND WHERE EITHER
MOTIVATES THE ATTACKER OR-- IS
DEFINITELY A CALL WE LEARNED
ON THE DESKTOP WORLD.
I THINK THAT IS A PRETTY
SHORT DELTA.
WE ARE RELEASING RAPID
UPDATES QUICKLY.
>> THIS ALL SOUNDS RELATED
TO DOWNLOADS, ARE YOU NOT
MAKING SCIENTIFIC CLAIMS
ABOUT --
>> I COULD GO, I COULD PUT
UP THE SLIDES UP LATER BUT
THIS IS BASED ON 60,000 RUNS
AND DOWNLOADS PER
APPLICATION WHICH HAS SOME
SELF-SELECTION AND SOME
SELECTION BIAS BECAUSE IT'S
NOT YOUR GRANDMA WHO IS
DOWNLOADING THIS APPLICATION
TO RUN IT, IT'S THE VERY
TECH SAVVY FOLKS.
AND MIGHT BE RUNNING CUSTOM
ROMS THAT ARE PATCHED
FURTHER.
AND THEN EXTRAPOLATED OUT
USING GOOGLE'S PUBLIC DATA
TO THE ENTIRE ANDROID
POPULATION SO IF WE SAW THAT
98% OF USERS RUNNING 2.3.3
ARE VULNERABLE AND WE KNOW
THAT 2.2.3 REPRESENTS 50% OF
THE ANDROID POPULATION, THEN

WE CAN EXTRAPOLATE OUT TO
THAT NUMBER.
SO I AM NOT A STATS MAJOR
AND I WOULDN'T HOLD THIS UP
TO A STATS PROFESSOR BUT
EVEN IF YOU LOOK AT THE PIE
CHARTS OF CONTRIBUTION THAT
GOOGLE PUTS OUT AND THE
NUMBERS ASSOCIATES WDZ THOSE
PIE CHARTS, AND CROSS
REFERENCE THAT WITH WHAT
PUBLICS HAVE BEEN DISCLOSED
AND EXPLOITING IN THE WILD,
YOU CAN SEE IT'S A
SIGNIFICANT PERCENTAGE.
>> ALEX OR JOHN, YOU WANT TO
JUMP IN ON THIS.
>> EXPAND ON THAT A LITTLE
BIT.
GOING BACK TO ALEX'S COMMENT
EARLIER, I THINK ARE YOU
TALK ON A SLIGHTLY DIFFERENT
SALE, ON THE CHIP LEVEL UP
TO THE TOP.
>> I'M TALKING ABOUT THE
PROBLEMS THAT I HAVE.
SO I WANT TO-- LET'S NARROW
IT DOWN TO JUST LIKE THE
SAND BOX TYPE
VULNERABILITIES.
AND I DON'T THINK WE'RE
QUITE IN A PLACE WHERE WE
SHOULD THROW OUR HANDS.
THERE ARE MANY EXAMPLES OF
APP SELL PROBABLY THE
KLEENEX AMPLE BUT PROBABLY
ALSO THE EASY EXAMPLE AM IF
YOU TAKE JUST ANDROID AND
LOOK AT THE OTHER
INTEGRATING DEVICES ON
ANDROID, GOOGLE'S OWN
DEVICES, THOSE ARE ALL-- VERY
GENEROUS.
AND GOING BACK TOTAL ZON
EXAMPLE, KINDLE DEVICE HAS
ALSO RECEIVED UPDATES VERY

QUICKLY.
WE'RE TALKING ABOUT HOW LONG
IT TAKES TO GET A PATCH.
IT'S REALLY NOT ANY
PARTICULAR DEVICE PROBLEM T
TOTALLY COMES DOWN TO HOW
MANY CHANGES.
>> AND SO YOU START RUNNING
THESE PROBLEMS WHERE THE
NEED TO COME FROM GOOGLE TO
AN OEM TO A CARRIER.
AND MOST CASES IT'S NOT EVEN
A TIME DELAY, IT'S THAT
THOSE PLANS OF COMMUNICATION
ARE SIMPLY BROKEN.
THE DEVICES LAUNCHED SIX
MONTHS AGO ARE ESSENTIALLY
END OF LIFE AND WILL NO
LONGER BE SEEING SECURITY
PATCHES BECAUSE THEY JUST
SIMPLY DON'T EXIST ANY MORE.
AND KEEP MAINTAINING THOSE
AND KEEPING THEM IN PLACE IS
DEFINITELY COSTLY AND
COMPLICATED BUT IT'S ALSO
SOMETHING THAT SHOULD BE
HAPPENING.
AND I THINK IT'S A LITTLE, I
AM GOING TO BE A LITTLE
CONTROVERSIAL HERE.
I REJECT THE PREMISE THAT WE
SHOULD WAIT UNTIL THERE'S
DATA SHOWING THAT A
SUFFICIENT NUMBER OF PEOPLE
HAVE BEEN EXPLOITED AND
HARMED BEFORE WE RELEASE
THAT.
WAITING UNTIL THERE'S
EVIDENCE OF HARM BEFORE WE
GO AN TRY TO CORRECT THE
PROBLEM IS REALLY A
DISSERVICE TO ALL.
AND IT IS NOT TO SAY THAT
IT'S-- IT IS ABSOLUTELY A
HARD PROBLEM BUT THERE ARE
PLACES THAT HAVE GOT IT

RIGHT.
AND I THINK WE SHOULD
ENCOURAGE MORE OF THAT.
>> ANYONE ELSE.
SO A COUPLE POINTS HAVE BEEN
MADE WITH.
ONE IS THE SUGGESTION THAT THE
ECOSYSTEM IS WAITING, IT'S NOT
PATCHING.
IS A PRIORITY NOW QUESTION IS,
CAN PATCHING ALWAYS HAPPEN
FASTER.
SURE IT CAN ALWAYS HAPPEN
FASTER.
IT CAN BE IMPROVED UPON.
IS IT PRIORITY FOR THE INDUSTRY,
YOU'LL SEE THAT NOT ONLY WHAT WE
PUBLISHED YOU'LL SEE THAT IN THE
WORK THAT WE'RE DOING WITHIN THE
CYBERSECURITY WORKING GROUP AND
BRINGING THAT FORWARD IN TO ALSO
THE WORK THAT WE'RE DOING ON THE
NATIONAL CYBERSECURITY FRAMEWORK
THAT WAS DIRECTED BY THE
EXECUTIVE BOARD.
MY POINT THERE IS THAT THE
SUGGESTED IT'S NOT PRIORITY THAT
IT'S NOT SOMETHING THAT THE
INDUSTRY IS FOCUSED ON I DON'T
THINK IS A FAIR REPRESENTATION
OF WHAT THE INDUSTRY IS DOING.
AND IN PARTICULAR I WOULD SAY
THAT THE LINES OF COMMUNICATION
ARE OPEN.
I KNOW THIS FOR A FACT BECAUSE I
WORK WITH THESE FOLKS ALMOST ON
A DAILY BASIS.
AND IT'S NOT A FAIR
CHARACTERIZATION.
BECAUSE AGAIN I KNOW FOR A FACT
THAT SECURITY IN PARTICULAR IS A
PRIORITY FOR THE CARRIERS AND
THEY PUT IT THROUGH AN EXPEDITED
PROCESS.
I'M NOT IN A POSITION TO
DISCLOSE THE PROCESS BUT THAT'S

PRY PRY TERRY TO EACH CARRIER.
THEY DO THIS EVERY DAY AND DO IT 24/7.
THAT'S WHY THEY HAVE THINGS THAT ARE CALLED NETWORK OPERATION CENTERS FOR SECURITY.
THAT'S WHY THEY HAVE CSOS AND VARIETY OF OTHER SECURITY MECHANISMS IN THEIR OVERALL STRUCTURES.
I HAVE TO TAKE ISSUE WITH IT NOT BEING PRIORITY BECAUSE IT IS.
NOW, CAN IT BE IMPROVED UPON, SURE IT CAN.
BUT IT'S GOT TO BE LOOKED AT IN THE CONTEXT OF THE DIFFERENT ECOSYSTEMS THAT HAVE FOB SUPPORTED.
ON PANEL TWO YOU SAW HOW MANY ECOSYSTEMS?
THERE WEREN'T JUST TWO.
BLACKBERRY, MICROSOFT AND APPLE EVER ALL DIFFERENT COMPANIES THEY DO THINGS DIFFERENTLY.
BUT YET ALL THAT HAVE HAS TO BE ACCOMMODATED IN ORDER TO SUPPORT A COMPETITIVE AND DIVERSE MARKETPLACE.
AGAIN THE INDUSTRY IS DOING EVERYTHING THAT IT CAN INCLUDING DOWN TO THE CHIP LEVEL IN TERMS OF THE ACTUAL FOUNDATION OF THE HOUSE IN TERMS OF THE HARDWARE TO MAKE SURE THAT WE'RE NOT DOING ANYTHING THAN COMPROMISE RELIABILITY.
BECAUSE AT THE END OF THE DAY THAT'S WHAT WE'RE FOCUSED ON.
>> I DON'T WANT TO DWELL ON THIS TOO MUCH LONGER, I THINK I HEARD YOU GUYS TALKING -- ALEX EITHER ONE OF YOU CORRECT ME WAS TALKING ABOUT TECHNICAL LINES OF COMMUNICATION LIKE ABILITY TO SEND THE SIGNAL TO THE PHONE MORE INFORMALLY ABOUT HUMAN

LINES OF COMMUNICATION, AM I RIGHT?
>> TAKE ANECDOTAL EXAMPLE.
MY FIANCE BOUGHT A DEVICE NINE MONTHS THROWING, THERE WAS AN ANDROID -- RELEASE AFTERWARDS, GOOGLE PATCHED IT.
SHE STILL WAITING ON A SECURITY UPDATE NINE MONTHS LATER THAT'S JUST ONE OF MANY SECURITY HOLES.
SHE'S IN -- ABSOLUTELY IN THAT 60% BUCKET THAT JOHN WAS TALKING ABOUT.
AND IN THE CURRENT STATE OF THE WORLD SHE WILL MOST LIKELY BUY A NEW PHONE BEFORE SHE RECEIVES A SECURITY PATCH.
YOU'RE ABSOLUTELY RIGHT IN THAT THERE IS NO KNOWN IN THE WILD THAT EXPLOITING THAT VULNERABILITY AS --
>> I CAN MAKE IT HAPPEN.
[Laughter]
>> I WOULD ADVISE YOU NOT TO I'M NOT YOUR LAWYER.
WHAT I WANT TO DO, I WANT TO END THIS ON TIME.
I'M GOING TO -- SINCE ALEX AND JOHN WANT TO JUMP IN THERE I'LL LET YOU SPEAK LAST ON THIS NEXT QUESTION.
IT'S AN OPEN ENDED QUESTION FRANKLY YOUR IF YOU JUST IGNORE ME ANSWER ANOTHER QUESTION.
THE QUESTION IS IF WE GOT THE BAND BACK TOGETHER IN FIVE YEARS AND WE DID THIS PANEL AGAIN, WHAT WOULD WE BE TALKING ABOUT, WOULD THINGS BE BETTER, WORSE, DIFFERENT, WOULD WE HAVE SOLVED ALL OF THE PROBLEMS.
AGAIN, IF YOU DON'T WANT TO ANSWER THAT THEN TALK ABOUT SOMETHING ELSE.
>> TOP OF MY WISH LIST IN THE MOBILE SECURITY SYSTEM.

I THINK WE NEED BETTER MECHANISM FOR PASSING DATA BETWEEN SANDBOX APPLICATIONS, THAT'S COMING FROM A PLATFORM ON A PLATFORM PERSPECTIVE.
WE'RE ACTIVELY WORK ON THAT.
THE STATE OF THE WORLD IS MUCH BETTER THAN IT WAS.
SECOND ITEM ON MY WISH LIST WE NEED TO GET MUCH BETTER ABOUT DELIVER SECURITY UPDATES TO THE ENTIRE ECOSYSTEM.
>> I TOUCHED ON THIS EARLIER BUT I THINK THAT PATCHING IS THE NUMBER ONE PROBLEM IN MOBILE SECURITY NOW OR AT LEAST HAS THE MOST IMPACT OR POTENTIAL IMPACT WHICHEVER WAY YOU WANT TO LOOK AT IT THE SOLUTION IS TO OPEN UP THE PLATFORM A LITTLE MORE AND PROVIDE THE ABILITY FOR THIRD PARTIES TO STEP IN PROVIDE SECURITY SERVICES AND ALLOW CARRIERS TO BRUSH THAT RESPONSIBILITY OFF THEIR SHOULDERS.
I DON'T THINK THEY WANT IT.
I DON'T KNOW IF THEY'RE CURRENTLY EQUIPPED TO DO IT.
AND I THINK THAT OPENING IT UP TO THE MARKET WILL BE THE MOST PRODUCTIVE AND EFFICIENT WAY FORWARD.
>> AGAIN, AT THE RISK OF TAKING ISSUE, THE MARKETPLACE IS OPEN, THERE ARE LOTS AND LOTS OF SECURITY COMPANIES THAT ARE IN THE BUSINESS OF PROVIDING SECURITY MOBILE DEVICES, A LOT OF THEM SIT ON THE GROUPS THAT WE HAVE WITHIN THE INDUSTRY.
SO FROM THAT PERSPECTIVE, AGAIN, I STRUGGLE WITH THE ISSUE OF OPENNESS BECAUSE AT ONE POINT SAYING THAT THE ECOSYSTEM IS TOO OPEN NOW WE'RE ADVOCATING FOR

IT.
PUTTING THAT ASIDE, I THINK IF
WE GET THE BAND BACK TOGETHER IN
FIVE YEARS, I THINK WE WILL BE
SURPRISED AT HOW THE REST OF THE
GLOBE HAS REALLY FOLLOWED THE
EXAMPLE OF THE UNITED STATES.
BECAUSE IT'S NOT GONE UNNOTICED
THAT AGAIN THE INFECTION RATES
IN THE UNITED STATES ARE WHERE
THEY ARE COMPARED TO OTHER
MARKETS.
BECAUSE I SEE THAT FROM
CARRIERS, I THAT FROM OEMs
EVEN WHOLE ISSUE OF CURATED AN
STORES.
I THINK WHAT WE'LL SEE IN FIVE
YEARS IS AGAIN HOW THE INDUSTRY
HAS EVOLVED TO ADDRESS BEST
PRACTICES AND STANDARDS ACROSS
THE BOARD.
ACROSS EVERY ELEMENT OF THE
ECOSYSTEM INCLUDING APPLICATION
DEVELOPERS.
AND IT WILL BE EASY TO FOLLOW.
I THINK FOR MOST PART BE
SURPRISED AT HOW EXPANSIVELY THE
MARKETPLACE HAS BECOME.
AGAIN BEING DRIVEN BY
APPLICATIONS AND EVERYTHING THAT
WE DO ON SMART PHONES, I ALSO
PREDICT IN FIVE YEARS EVERYBODY
WILL WONDER WHAT A PC IS.
WITH THAT THANK YOU.
>> SURE.
ALEX?
>> I'M GOING TO TAKE YOU UP ON
THE OFFER BASE YOU CANNILY TALK
ABOUT SOMETHING ELSE.
I'M NOT GOING TO, IN PART I
DON'T WANT TO TRY TO PREDICT THE
FUTURE I STILL REMEMBER HOW FAR
IN TERMS OF PREDICTING WHAT
WOULD BE HAPPENING.
ALSO DISAGREE WITH JOHN AND ALEX
ON SOME OF THE -- PATCHING

EVERYTHING AND MITIGATING
VULNERABILITY.
IN A WAY IT'S AN APPROACH THAT
WE -- OUR COMMUNITY RIDICULES
WHEN IT COMES TO NATIONAL
SECURITY IN THE AIRPORT SECURITY
THEATER.
IT'S NOT THE APPROACH THAT WE
TAKE IN OUR DAILY LIVES.
I'M GUESSING THAT OUR HOUSE IS
FULL OF VULNERABILITIES, WE
DON'T HAVE BARS ON OUR WINDOWS,
STONE WALLS, MOATS WITHDRAW
BRIDGES, THOSE ARE DENIABILITIES
THAT ARE REALLY IMPROBABLE --
REALLY UNLIKELY TO BE EXPLOITED
WE DON'T BOTHER PATCHING THEM.
WHEN I LOOK AT THE MOBILE
ECOSYSTEM YES THERE ARE
VULNERABILITIES.
SAME TIME LOOK AT POTENTIAL
IMPACT ON USERS IF ALL WERE
PATCHED BY THE END OF PANEL
TODAY, THE PERCENTAGE OF USERS
THAT WOULD ACTUALLY EXPERIENCE A
DEGRADATION AND UNWELCOME
BEHAVIOR IS GOING TO BE NECK
RIDGABLE.
NOT GOING TO IMPACT MOST OF THE
USERS.
AS INDUSTRY WE'RE TRYING TO LOOK
AT THE DATA FOCUS ON THINGS
WHERE WE CAN MAKE THE MOST
IMPACT.
THAT'S NOT TO SAY PATCHING IS
NOT IMPORTANT PROBLEM TO SOLVE.
WE HAVE THE ABILITY TO REACT
BECAUSE WE CAN'T PREDICT WHAT IS
GOING TO HAPPEN.
IT IS SOMETHING THAT WE'RE
WORKING TO ADDRESS.
BUT IT IS ESPECIALLY DOWN AT THE
LOWER LAYERS, IT'S VERY
CHALLENGING PROBLEM.
IF I HAVE TIME --
>> REALLY BRIEF.

>> COUPLE OF YEARS AGO MY SON WAS ASKING ME ABOUT MY JOB AND I WAS TRYING TO MAKE IT INTERESTING TO A 10-YEAR-OLD I DESCRIBED SOFTWARE AND MAL WEAR AND EXPLOITS AND TROJANS AND VIRUSES ALL THE TERMS THAT LUCKILY WE PICK THAT SOUND COOL FOR A 10-YEAR-OLD.
AND HE HAD REALLY UNEXPECTED REACTION.
HE ASKED ME, SO WITH SO MANY THINGS THAT GOING WRONG ON THE INTERNET SHOULD I BE YOUTHING A COMPUTER, SHOULD I GO ON THE INTERNET?
IT'S NOT AT ALL THE REACTION THAT I WAS HOPING FOR.
IF I WAS A LITTLE BIT SHOCKED, I THOUGHT ABOUT IT I TOLD HIM, LOOK, EVERYBODY TIME YOU LEAVE YOUR HOUSE THAT THING -- BAD THINGS CAN HAPPEN, THERE ARE BAD PEOPLE OUT THERE WHO WILL TRY TO HURT YOU, YOU CAN GET IN TO ACCIDENTS, I TRIED TO EXPLAIN IT TO A 10-YEAR-OLD.
THERE ARE DISEASES, LOTS OF THINGS CAN GO WRONG BUT WE DON'T STAY LOCKED UP IN OUR HOUSES, REALITY IS, WE GET MUCH MORE VALUE OUT OF COMMUNICATING WITH OTHER PEOPLE.
THESE DEVICES ARE SIMILAR.
TODAY WE GET MUCH MORE VALUE OUT OF USING THEM, THAN THE RISK -- SECURITY IS NOT ABSOLUTELY GREAT IT'S A BENEFIT TO RISK RATIO.
THESE DAYS THE PACE OF INVASION SO HIGH THAT WE'RE ADDING MUCH HIGHER RATE.
>> ENDING NOTE THAT IS SIMULTANEOUSLY VERY DARK AND ALSO HOPEFUL --
>> IT'S HOPEFUL.
>> PLEASE JOIN ME IN THANKING

THE PANEL.
[APPLAUSE]
LET'S GIVE YOU FIVE MINUTES
BACK.
3:20 DOES THAT SOUND OKAY?