; 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.

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

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 NEXTTO
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.

T 12.05 0 TRP <</MC1(Y T)-1<</MCIMC /Y 11(NG T)-11(O HsND-MCID 1 >>BDC 0OP EMC /P0OP E8(E)-1(AD

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 VIEWAND 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

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

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 FORACCESS 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,

TO DO.
WHEN YOU NOTICE SOMETHING
THAT ISN'T SO GOOD, THEN YOU
PATCH.

(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.

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 SPS78KRSÍ‘Ká ÜÑ a]b %]. Ú]b % RGHT TE WEHAV(E)-1(OV(E)-1(R)-5(2,)-25,)-20,.1 /(E)-1(M

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

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

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

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--

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

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 SAI D 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 EVERYTHNG
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

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/OP <</MTw 14.34 0 Td ( )-10(2(L)9(E)-)11(T)-1(T)-11(HR)-5(OUGH/OO)-10(T)--10( )]<

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

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
TH >>BDC 2jY4.42 -1.15 Td [(S)-6((TA)192 0 YF)4(W)11D1WHAAF
IHOE2 02.

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

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

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

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
ACROSSTHE-BOARD.
AND IF EVERYTHING GOES
ACCORDING TO PLAN, THE
CYBERSKOOURT FRAMEWORK WILL
BE DONE BY F-10(OW8w 17.0 IAHC /P1(,)+2T)-10(IO0(OW B)5(YX0 Tc 0 Tw 15.53 0 T9 ( )Tj EMC

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

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 --
>> SOLET 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

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 THEIRDATA, 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 SIMPLEAPPLICATION AND SAY INSTA GRAM TO A LARGE NUMBER OF USERS WITHOUT THE TYPICAL

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 BULD 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 A BOUT-- 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 ISQUITE 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

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

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.

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

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.

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 ISSAYING
THERE IS NOT NECESSARILY AN
URGENT TH Tc 0.21Oj-5(-4(-1.15 Td [O(EO 0.012SI)11 G(P)-162)17 S 1.ASTA)0(Td (S)TN4 MC-1(HAT)-1

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

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.

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

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 THEFAHENCT P9 -1.15 Td [(P)-6(AT)-1(C)-5(18.002 -D)-10(O
YOU'L PR10(N T)-1(HAT)-1(T)-1(9(S)-1J 0 Tc 0 Tw 16.21 0 Td ( )Tj E16.21(Y)-10(NOW)-2T)-1(HE)-1(I)11(NDU

PRY PRY TERRY TO EACH CARRIER.
THEY DO THIS EVERY DAY AND DO IT
24/7.
THAT'S WHY THEY HAVE THINGS THAT

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 0.00.57 -1DV1H.01 Tw -15.57 -1. >>BDC-1.1j EMC /P <</MCID 34 0 Tw 18.9Tc 0 Tw 18.64

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.

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 THEMOST 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, ITRIED 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,

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