FTC Fall Technology Series: Ransomware
September 7, 2016
Segment 2
Transcript

;;;;Panel 2

>> IF EVERYONE CAN FIND THEIR

WAY BACK TO THEIR SEATS, WE'LL

GET STARTED IN JUST A MINUTE.

SO WELCOME BACK.

I HOPE EVERYONE WAS ABLE TO GRAB

SOME COFFEE.

I KNOW IT'S THE AFTERNOON, BUT

WE'VE GOT A COUPLE OF EXCITING

PANELS LEFT, AND I HOPE YOU'RE

ENJOYING THE PROGRAM SO FAR.

I'M BEN ROSSEN, I'M AN ATTORNEY

IN THE DIVISION OF PRIVACY AND

IDENTITY PROTECTION HERE, AND

I'M VERY EXCITED TO INTRODUCE

OUR NEXT PANEL WHICH WILL

DISCUSS BEST DEFENSE TACTICS

AGAINST RANSOMWARE.

SO WITH US TODAY, AND AGAIN I'M

NOT GOING TO GO THROUGH THE FULL

BIO BUT I ENCOURAGED YOU TO LOOK THROUGH THE PAPERS IN FRONT OF YOU.

WE HAVE KEITH McCAMMON, CHIEF SECURITY OFFICER/CO-FOUNDER, RED CANARY, WE SPECIALIZES IN ENDPOINT SECURITY AND THREAT DETECTION.

WE HAVE LORRIE CRANOR, CHIEF TECHNOLOGIST, F.T.C., ON LEAVE FROM CARNEGIE MELLON UNIVERSITY WHERE SHE IS A PROFESSOR OF COMPUTER SCIENCE, ENGINEERING AND PUBLIC POLICY.

WE HAVE BILL WRIGHT, DIRECTOR OF GOVERNMENT AFFAIRS, SYMANTEC.

HE HEADS UP THE NORTON CYBERSECURITY INSTITUTE THERE.

AND WE HAVE CHAD WILSON, DIRECTOR OF INFORMATION SECURITY, CHILDREN'S NATIONAL MEDICAL CENTER HERE IN WASHINGTON, D.C.

HE LEADS THE HOSPITAL'S NETWORKS

CYBERSECURITY STRATEGY AND

IMPLEMENTATION.

SO I'M REALLY EXCITED TO HAVE

THIS PANEL BACK WITH US TODAY

AND HOPE THIS WILL BE AN

INTERESTING PANEL.

SO TO GET STARTED, THE GOAL WITH

THIS IS TO KEEP THIS

CONVERSATIONAL, AND I DO

ENCOURAGE YOU, IF YOU HAVE ANY

QUESTIONS, PLEASE FILL OUT

COMMENT CARDS AND PASS THEM OUT.

WE'LL TRY TO GET TO THEM AT THE

END OF THE SESSION.

EARLIER TODAY, WE'VE HEARD A LOT

OF DOOM AND GLOOM AND RANSOMWARE

AND HOW PREVALENT IT IS AND HOW

QUICKLY IT'S GROWN.

BUT I'M HOPING THERE IS POSITIVE

LIGHT WE CAN SHED DURING THIS

PANEL.

I'M HOPING TO TALK ABOUT

PREVENTION AND SPECIFICALLY
WHETHER THERE ARE ANY STEPS THAT
BUSINESS AND INDUSTRY CAN TAKE
TO PREVENT ATTACKS, AND WE'LL
TALK ABOUT CONSUMERS NEXT, BUT
THIS IS A GOOD PLACE TO START.
SO, KEITH, I'LL TURN IT OVER TO
YOU.
>> YEP, SURE.
APPRECIATE THE OPPORTUNITY AND
THANK YOU ALL FOR COMING.
SO ONE OF THE WORDS THAT'S
CONTINUED TO COME UP TODAY AS WE
WERE TALKING EARLIER AS A PANEL
ABOUT SOME OF THE THEMES WE
WANTED TO HIT, HYGIENE IS THE
THING THAT CONTINUES TO COME UP
AND I THINK WE'LL PROBABLY SEE
THAT BLEED OVER, YOU KNOW,
WHETHER THEY'RE TALKING ABOUT
BUSINESSES OR CONSUMERS.
THAT'S A BIG PART OF IT.
WHEN IT COMES TO RANSOMWARE,

WHICH IS THIS KIND OF HYBRID
TECHNICAL AND SOCIAL PROBLEM, IT
REALLY IS EQUAL PARTS HYGIENE ON
THE PART OF IN TERMS OF
AWARENESS, ONGOING EDUCATION AND
SOME OF THAT CAN BE, YOU KNOW,
STRICTLY INFORMATION PUSHY
TECHNOLOGISTS TO CONSUMERS OR
BUSINESSES.
SOME IS IN THE FARM OF TECHNICAL
CONTROLS AND THINGS LIKE THAT,
BUT HYGIENE IN GENERAL THING IS
PROBABLY, IF I DEPICT ONE -- IF
I HAD TO PICK ONE THING, YOU
KNOW, CHECK YOUR E-MAILS, IF YOU
DON'T EXPECT IT, DON'T OPEN IT.
TEACH PEOPLE TO LOOK FOR THE
GREEN BAR AT THE TOP, MAKE SURE
THE NAME OF THE SITE YOU'RE
VISITING MATCHES THE NAME YOU
EXPECT TO SEE.
REALLY BASIC THINGS LIKE THAT.
>> SO, YEAH, IN TALKING ABOUT

HYGIENE, I GUESS HOW WOULD YOU
BREAK THAT DOWN EVEN FURTHER
BEYOND JUST CHECKING YOUR EMAIL?
ARE THERE OTHER ASPECTS IN TERMS
OF, YOU KNOW, FOING WHAT'S
CONNECTED TO THE NETWORK AND
IMPLEMENTING SECURITY STANDARDS
ON THE BACK END?
ARE THERE STANDARD THINGS YOU
THINK REALLY SHOULD BE ON THE
RADAR OF PEOPLE THESE DAYS?
>> YEAH, SURE.
SO FROM A CORPORATE PERSPECTIVE,
AGAIN, HYGIENE MEANS DIFFERENT
THINGS TO DIFFERENT PEOPLE IN.
THAT REGARD, UNDERSTANDING WHAT
YOU HAVE, WHICH IS JOB ONE, I
THINK ONE OF THE MOST COMMON
PROBLEMS WE SEE WHEN WE WALK
INTO ORGANIZATIONS, PARTICULARLY
LARGE ONES, THEY THINK THEY HAVE
2000 COMPUTERS, THEY REALLY HAVE
THREE.

WE'VE SEEN CASES WHERE THEY HAVE
50, THEY REALLY HAVE 60.
UNDERSTAND WHAT'S THERE AND THE
SCOPE OF YOUR RESPONSIBILITY,
WHICH IS THE BIG PIECE, TOO, SO
A LOT OF THE PRODUCTS AND A LOT
OF THE EDUCATION, A LOT OF THE
TRAINING THAT I THINK INDUSTRIES
RECEIVED OVER THE YEARS, IT'S
BEEN REALLY, REALLY FOCUSED ON
P.C.s.
NOW YOU'VE, YOU KNOW, GOT A
LARGER MAC POPULATION OUT THERE,
YOU'VE GOT MULTIPLE DEVICES PER
USER, SO IT'S GETTING TO BE
REALLY COMMON.
IT WOULD BE INTERESTING TO HEAR
YOUR TAKE ON EDUCATION WHERE YOU
THINK YOU LOOK AT COLLEGE
CAMPUSES AND YOU'VE GOT ON
AVERAGE FOUR TO FIVE DEVICES PER
STUDENT.
SO FROM AN ORGANIZATIONAL

PERSPECTIVE, TAKE STOCK OF THE
SCOPE OF YOUR EXPOSURE,
UNDERSTAND WHAT YOU'VE GOT,
UNDERSTAND WHAT CONTROLS YOU CAN
AND CAN'T PUT IN PLACE AND BE
REALLY VIGILANT ABOUT ITEMIZING
THOSE THINGS, RESEARCHING THOSE
RISKS AND MITIGATING WHAT YOU
CAN AND EDUCATING WHERE YOU CAN
TO TECHNICALLY PREVENT.
>> JUMPING IN HERE.
IT'S REALLY HARD TO OVERSTATE
THE NECESSITY OF GOOD CYBER
HYGIENE.
AT LEAST ON THE DATA BREECH
SIDE, ONLINE TRUST ALLIANCE PUT
OUT A STUDY ABOUT A YEAR AGO
THAT SAID ABOUT 90% OF ALL
BREACHES COULD BE SOLVED BY SOME
PRETTY BASIC CYBER HYGIENE, SO
THAT'S A PRETTY INCREDIBLE STAT.
YOU KNOW, I THINK WE WOULD ALL
AGREE THAT, AT LEAST WITH

RANSOMWARE, ONCE YOUR DATA IS ENCRYPTED, IT'S PRETTY NEAR IMPOSSIBLE TO GET BACK, SO THE FOCUS REALLY NEEDS TO BE ON THE PREVENTION SIDE.

SO USING ALL OF THOSE TECHNOLOGIES AT YOUR ENDPOINT SECURITY PRODUCT HAS, SO EMAIL SECURITY, INCLUDING AUTHENTICATION POSSIBLY OF INBOUND, INTRUSION PREVENTION, WEB BROWSER PROTECTION, EXPLOIT PROTECTION, PATCH, PATCH, PATCH.

YOU KNOW, GET THE EASY ONES OFF THE TABLE.

TRY TO COVER THOSE VULNERABILITIES, THE KNOWN VULNERABILITIES.

BUT MOST IMPORTANT HAS TO BE TO TRAIN THE END USERS.

THE VAST MAJORITY OF THE END USERS ARE GETTING FOOLED BY THE SAME SORT OF SOCIAL ENGINEERING

PHISHING ATTACKS.

ALWAYS HAVE BACKUP IN PLACE.

I'M SURE YOU'VE HEARD THAT 15

TIMES TODAY.

>> YEAH.

I WOULD ONLY ADD TO THAT, IT'S A

TECHNICAL PROBLEM.

THEY'RE ATTACKING US

TECHNICALLY.

THERE ARE A LOT OF THINGS THAT

YOU CAN DO FROM A PREVENTION

PERSPECTIVE BY INVESTING IN

TECHNOLOGY THAT ACTUALLY DOES

SOME OF THAT HYGIENE UP FRONT

FOR YOU.

SO THERE ARE THINGS YOU CAN DO

THAT DON'T EVEN ALLOW THE USE

TORE SEE AN INVOICE .PDF, THAT

THEY'RE NOT IN FINANCE, THEY

SHOULD NEVER BE GETTING THOSE.

SO UNDERSTANDING YOUR BUSINESS

AND MARRYING THAT WITH SOME OF

YOUR TECHNICAL CONTROLS WOULD

REALLY HELP DO SOME OF THAT
HYGIENE UP FRONT AND REMOVE A
GOOD SECTION OR A GOOD
PERCENTAGE OF WHAT THAT THREAT
IS BEFORE IT EVEN GETS IN, AND
THEN YOU HAVE TO THINK ABOUT, I
DON'T CARE, WELL, IF I HAVE
INVESTED X IN PREVENTION, WHAT
DO I HAVE TO INVEST IN INCIDENT
RESPONSE AND BEING ABLE TO KNOW
AND MEASURE WHAT MY ACTUAL
RESPONSE HAS TO BE AND WHAT I
HAVE TO DO TO RESPOND TO AN
INCIDENT, WHETHER THAT'S RESTORE
BACKUPS, TIME IT TAKES TO DO
THAT OR JUST WIPE THE DEVICE AND
KEEP ON MOVING.
>> SO, YOU KNOW, ONE OF THE
THINGS I'M CURIOUS ABOUT, WE'VE
HEARD A LOT ABOUT -- RANSOMWARE
ITSELF IS NOT A NEW PROBLEM.
OBVIOUSLY, PEOPLE HAVE BEEN
FACING MALWARE FOR A LONG TIME.

IS THIS ANY DIFFERENT FROM OTHER
MALWARE OR ARE YOU REALLY
APPLYING THE SAME BASIC
TECHNIQUES TO MALWARE AS THE
RANSOMWARE THREAT?
>> WELL, I THINK, WHILE THERE
ARE DEFINITELY SOME THINGS THAT
ARE DIFFERENT ABOUT IT AS FAR AS
THE CONSEQUENCES, AS FAR AS HOW
DO WE TRAIN PEOPLE TO AVOID IT,
I THINK IT'S A LOT OF THE SAME
SORTS OF THINGS.
SO, YOU KNOW, WE HAVE BEEN
TRYING TO TRAIN PEOPLE TO AVOID
PHISHING ATTACKS AND MALWARE FOR
15 YEARS NOW AND I THINK IT'S
PRETTY MUCH THE SAME KIND OF
THINGS WE WANT TO TEACH THEM.
THERE IS THE ASPECT OF, HEY, YOU
COULD LOSE ALL YOUR FILES, WHICH
IN SOME WAYS MAY BE EVEN A
SCARIER CONSEQUENCE TO PEOPLE.
SO I THINK IT'S WORTH TALKING

ABOUT THAT AND HOPEFULLY RAISING
PEOPLE'S INTEREST IN DOING
SOMETHING ABOUT IT BECAUSE, YOU
KNOW, THEY DON'T WANT THAT
CONSEQUENCE.
>> WHEN YOU ASK ABOUT THE
SPECIFIC DIFFERENCES OR WHETHER
IT'S DIFFERENT THAN THINGS WE'VE
SEEN IN THE PAST, IF YOU WATCH
THE PRESENTATIONS EARLIER, THE
MOST INTERESTING THING IS YOU
CAN KIND OF DRAW A LINE DOWN THE
MIDDLE AND DIFFERENTIATE
INFECTION VECTORS FROM PAY
LOADS.
SO RANSOMWARE, JUST A NEW PAY
LOAD.
IT HAPPENS TO BE THE ONE WHERE
THERE IS A STRONG FINANCIAL
INCENTIVE SO WE'RE SEEING A LOT
OF VELOCITY BEHIND IT.
THE INFECTION VERDICT SIDE
HASN'T CHANGED AT ALL.

I SHOULDN'T SAY THAT.

IT CONTINUES TO EVOLVE, SO THERE

IS CAT AND MOUSE BETWEEN THREAT

ACTORS, TECHNICAL DEFENDERS,

YOUER OF EDUCATION.

SO BAD EMAIL, BAD WEB SITE.

THAT'S THE OVERWHELMING MAJORITY

OF IT.

YOU HAVE A SLIVER OF RISK

ASSOCIATED WITH THINGS LIKE

REMOVAL MEDIA, BUT THAT IS

REALLY A ROUNDING ERROR, WHEN

YOU LOOK AT WHAT'S GOING ON

RELATED TO RRMDZ AND THE OTHER

CRIMEWARE THREATS -- RELATED TO

RANSOMWARE AND THE OTHER

CRIMEWARE THREATS.

SO IT'S MORE EVOLUTIONARY RATHER

I DON'T THINK WE'RE ADVISING

PEOPLE TO DO ANYTHING NEW, WITH

THE EXCEPTION OF PROBABLY

INCREASED FOCUS ON BACKUPS

BECAUSE DATA LOSS IS A NEW

PROBLEM AND IT USED TO BE A
BUSINESS CONTINUITY PROBLEM AND
NOW IT'S A CONSUMER PROBLEM.
WITH THE EXCEPTION OF THE DATA
LOSS ASPECT, THE RANSOMWARE, THE
VECTORS HAVEN'T CHANGED, THE PAY
LOADS CONTINUE TO EVOLVE, BUT
THEY'RE NOT EVOLVING SO FAST
THAT WE'RE HAVING TO COME UP
WITH NEW WAYS TO TRAIN PEOPLE OR
EVEN NECESSARILY COMING UP WITH
A LOT OF NEW TECHNICAL DEFENSES.
THEY'RE EVOLVING ALONG WITH IT.
WE DON'T HAVE TO DO ANYTHING
REVOLUTIONARY TO PREVENT IT.
WE NEED TO EXECUTE ON THE THINGS
WE HAVE BEEN ASKING PEOPLE TO DO
FOR A LONG TIME.
>> ONE VERY OBVIOUS DIFFERENCE
BETWEEN MALWARE AND RANSOMWARE
AND PERHAPS THE SILVER LINING
YOU'RE LOOKING FOR IS RANSOMWARE
LETS YOU KNOW YOU HAVE BEEN

INFECTED UNLIKE TRADITIONAL

MALWARE.

SO THERE IS YOUR SILVER LINING.

>> LET'S TALK A LITTLE MORE

ABOUT BACKUPS BECAUSE THAT'S

PROBABLY THE IF YOU REMEMBER ONE

QUESTION WE'VE GOTTEN.

IS THERE ANYTHING PEOPLE SHOULD

KNOW ABOUT HOW TO BACKUP

EFFECTIVELY AND HOW TO BE ABLE

TO RELY ON YOUR BACKUPS SO IF

YOU GET HIT WITH RANSOMWARE, YOU

DON'T NEED TO WORRY ABOUT IT.

IF HE NEEDS A PAY, FALL BACK ON

RELIABLE BACKUPS.

BUT ARE THERE ISSUE WITH A

VARIANT THAT WILL LIE IN WAIT

AND CREEP INTO YOUR BACKUPS OVER

TIME?

WHAT STEPS DO PEOPLE NEED TO

TAKE TO BE IN POSITION OR DO

THEY JUST FALL BACK?

>> FROM A BACKUP PERSPECTIVE,

YOU HAVE TO BACKUP ON A ROUTINE
SCHEDULE SO YOU KNOW WHEN YOUR
LAST BACKUP IS THAT YOU CAN
REVERT BACK TO.
BUT YOU ALSO HAVE TO KNOW WHAT
DATA IS IMPORTANT TO BACK UP.
NOT EVERYTHING NEEDS TO BE
BACKED UP.
IT ONLY NEEDS TO BE BACKED UP IF
IT'S IMPORTANT TO YOU, YOUR
BUSINESS OR WHERE YOU'RE HEADED
WITH A PARTICULAR PROJECT OR
WHAT YOU'RE WORKING ON.
AND THERE IS MULTIPLE DIFFERENT
WAYS THAT YOU CAN BACK UP,
WHETHER THAT'S OVER THE NETWORK,
THE WEB, CLOUD.
BUT I THINK THE MOST IMPORTANT
THING IS UNDERSTANDING YOUR
BUSINESS.
IT STARTS WITH THE BUSINESS.
THAT'S WHAT THEY'RE
INTERRUPTING.

THEY'RE TRYING TO HOLD THE DATA
HOSTAGE, AND IT'S IMPORTANT TO
YOU AND IMPORTANT TO YOUR
BUSINESS.
THAT'S WHERE THE INCENTIVE COMES
FROM.
AND IF YOU MAKE SURE THAT THAT
IS -- THAT RISK IS MITIGATED
WITH GOOD BACKUP METHODOLOGIES,
YOU'VE TAKEN AWAY THAT
INCENTIVE.
>> I AGREE BACKUP IS ABSOLUTELY
CRUCIAL.
I DON'T THINK YOU CAN SEE IT AS
A COMPLETE PANACEA.
THERE ARE CHALLENGES WITH ANY
SORT OF BACKUP STRATEGY.
SPECIFIC TO RANSOMWARE, AT
LEAST, WE ARE SEEING ATTACKERS
GOING AFTER THE BACKUP AND WE
EXPECT THAT TREND TO KIND OF
CONTINUE.
MORE AND MORE OF THESE THREATS

WILL ADD SOMETHING TO THE CODE L
ADD SOMETHING TO HELP SORT OF
DISRUPT YOUR ABILITY TO RECOVER
VIA YOUR BACKUP, AND THAT'S KIND
OF WHERE WE SEE THIS GOING IN
THE FUTURE.
>> SO HOW ABOUT THE POSSIBILITY
OF RANSOMWARE GOING INTO THE
CLOUD?
THAT WAS ONE THING THAT WE HEARD
A QUESTION ABOUT EARLIER.
YOU KNOW, FOR A LOT OF PEOPLE,
ESPECIALLY CONSUMERS WHO MAY
JUST RELY ON DROP BOX OR GOOGLE
DRIVE TO KEEP THEIR DOCUMENTS
SAFE, IS THAT SOMETHING PEOPLE
NEED TO WORRY ABOUT OR ARE THERE
OTHER STEPS PEOPLE SHOULD BE
TAKEN?
>> I'LL TAKE A STAB AT IT.
SO I THINK SOME OF THE
DISCUSSION EARLIER ABOUT BACKUPS
WAS SPECIFICALLY RELATED TO HOW

EASY IT IS TO ACCESS THEM.

IF YOU CAN OPEN YOUR COMPUTER

AND GET TO ALL OF YOUR BACKUP

FILES RIGHT NOW, THEY PROBABLY

WON'T BE OF MUCH USE TO YOU

BECAUSE MALWARE AND RANSOMWARE

IN PARTICULAR CAN ACCESS THEM,

TOO.

SO IF YOU START THERE, GETTING

THEM OFF YOUR COMPUTER TO

SOMEPLACE ELSE THAT'S NOT

CONNECTED AS A DRIVE AND READILY

ACCESSIBLE TO ANY PERSON OR

THING THAT USES YOUR COMPUTERS

WILL HELP.

IT'S AN ADVANTAGE.

SPECIFICALLY RELATED TO THE

CLOUD-BASED BACKUPS, THE CLOUD

PROVIDERS KIND OF HAVE THE SAME

ADVANTAGE ALL THE BIG SASS

OFFERINGS DO.

THE ADVANTAGE OF A SASS IS THEY

CAN BE REALLY GOOD AT ONE THING

AND IF THEY IDENTIFY A THREAT,
TAKE GOOGLE FOR EXAMPLE, JUST
PICKING THEM OUT, BUT THEY'RE
AWARE IT'S A THREAT, THEY CAN --
THEY'VE GOT THE RESOURCES TO
FIGURE OUT THOUSAND MITIGATE
THAT FOR THEIR CUSTOMERS.
THEY ONLY HAVE TO MITIGATE IT
ONCE AND THEY CAN PROTECT TENS
AND HUNDREDS OF MILLIONS OF
PEOPLE.
SO USING A SOLUTION LIKE THAT,
PARTICULARLY ON THE CONSUMER
SIDE, YOU'VE GOT A MUCH GREATER
CHANCE OF SUCCESS THAN TRYING TO
GO IT ON YOUR OWN, KEEP ON TOP
OF ALL THE POTENTIAL PROBLEMS,
KEEP ON TOP OF THE EVOLUTION OF
MALWARE AND THE NEW AND CLEVER
WAYS THEY WILL TRY TO GET TO
YOUR BACKUPS.
SO IT'S, YOU KNOW, TO KIND OF
TIE IT BACK TO BUSINESS, IT'S

RISK TRANSFERENCE.

SO YOU CAN TRANSFER SOME OF THAT

RISK TO YOUR PROVIDER IN HOPES

THEY CAN DO A BETTER JOB OF

PROTECTING YOU THAN YOU CAN

PROBABLY PROTECT YOURSELF.

>> SO LET'S TALK A LITTLE BIT

MORE ABOUT CONSUMERS, BECAUSE I

THINK A LOT OF CONSUMERS WHO ARE

SORT OF IN THE CROSSHAIRS OF

THIS AND REALLY MIGHT HAVE NO

IDEA WHAT TO DO IF THEY GET HIT,

YOU KNOW, WE'VE TALKED ABOUT

BACKUPS, CYBER HYGIENE, BUT

AMONG THAT IS THERE ANY ONE

SINGLE THING THAT CONSUMERS

COULD DO TO HELP PROTECT AGAINST

THIS THREAT?

>> WELL, SO I THINK THE FIRST

THING IS TO BE AWARE OF IT.

I THINK A LOT OF CONSUMERS ARE

NOT AWARE.

IN FACT, I WAS TALKING TO SOME

FAMILY MEMBERS YESTERDAY AND
TELLING THEM I WAS GOING TO BE
SPEAKING AT THIS WORKSHOP TODAY.
AND SOME SAID RANSOMWARE, WHAT'S
THAT?
SO I THINK TO START IS BEING
AWARE.
BUT THEN I THINK THE THINGS THAT
WE HAVE BEEN TEACHING TO AVOID
PHISHING AND MALWARE ABOUT, YOU
KNOW, BEING CAREFUL ABOUT
CLICKING ON LINKS, BEING CAREFUL
ABOUT OPENING ATTACHMENTS, YOU
KNOW, BEING CAREFUL -- I GUESS
THE NEWER THING NOW WITH MOBILE
APPS, WHEN YOU GO TO APP STORES,
ABOUT WHAT APPS YOU DOWNLOAD.
SO A LOT OF THOSE TYPES OF CYBER
HYGIENE THINGS WE HAVE BEEN
TRYING TO TEACH FOR A WHILE ARE
REALLY IMPORTANT AND I THINK
CONSUMERS WHO ARE NOT YET
FAMILIAR WITH THIS, THERE IS ALL

SORTS OF RESOURCES ONLINE THAT
HAVE THESE ONLINE SAFETY TIPS
AND VIDEOS, INCLUDING THEORY AT
THE F.T.C.'S WEB SITE, BUT THERE
ARE LOTS OF OTHER GOOD PLACES AS
WELL.
>> SO ONE QUESTION.
IF YOU'RE A BUSINESS THAT'S
HOLDING CONSUMER DATA AND AT
RISK OF RANSOMWARE, TO WHAT
EXTENT DO YOU ALSO HAVE TO WORRY
ABOUT RANSOMWARE ACTUALLY
INFILTRATING THE DATA, STEALING
THE DATA AS WELL AS JUST LOCKING
YOU OUT OF IT?
IS THAT A CONCERN?
>> SO I'LL ANSWER THAT.
THE ANSWER IS YES, IT IS A
CONCERN.
IF YOU'RE HOLDING SENSITIVE DATA
THAT'S OTHER PEOPLE'S DATA, FOR
EXAMPLE THE GOVERNMENT HAS MY
DATA, I HAD A SECURITY CLEARANCE

ONCE, THEN IT'S REALLY IMPORTANT
TO MAKE SURE THAT THAT DATA
STAYS PROTECTED.
YOU HAVE TO BUILD THAT TRUST
WITH THE PEOPLE THAT YOU HAVE
THAT DATA WITH AND THAT YOU'RE
HOLDING THAT DATA FOR.
SO IF YOU'RE AT RISK OF
RANSOMWARE OR ANY OTHER MALWARE,
MEANING YOUR COMPUTER SYSTEMS
ARE CONNECTED OR THAT DATA IS A
TARGET, IF YOU HAPPEN TO HAVE AN
AIR GAP SYSTEM, MALWARE CAN JUMP
AIR GAPS AS WELL.
SO YOU NEED TO MAKE SURE THAT
YOU'RE DOING THE CYBERHYGIENE,
YOU'RE DOING THE THINGS
NECESSARY TO PROTECT THAT DATA
AND CHECKING IT OFTEN.
YOU HAVE TO KNOW -- ONE OF THE
THINGS WE FOCUS ON AT CHILDREN'S
IS IF YOU CAN'T SEE IT, YOU
CAN'T PROTECT IT.

YOU HAVE TO MAKE SURE YOU KNOW
WHERE THE DATA IS, WHAT SYSTEMS
ARE USED TO ACCESS THE DATA,
WHO'S ACCESSING IT AND WHAT
THEY'RE DOING.
THAT'S THE BASICS OF SECURITY.
IF YOU'RE NOT DOING THAT AS A
BUSINESS, THEN YOU'RE NOT REALLY
TAKING THE NECESSARY STEPS TO
RETAIN THAT TRUST AND CONFIDENCE
OF THE PEOPLE YOU HAVE THE DATA
FOR.
>> AND THEN IF YOU FIND YOURSELF
INFECTED, YOU NEED TO DO THE
BEST YOU CAN TO SORT OF ISOLATE
THAT COMPUTER BEFORE THE
RANSOMWARE CAN ATTACK NETWORK
DRIVES THROUGH THE ACCESS, USE
YOUR ENDPOINT PROTECTION MANAGER
TO UPDATE THOSE VIRUS
DEFINITIONS AS FAST AS POSSIBLE
AS WELL.
>> IF YOUR DATA IS ENCRYPTED,

ARE YOU BE ABLE TO RELY ON THE
FACT IT'S ENCRYPTED AND YOU
DON'T NEED TO WORRY ABOUT IT?
DOES THAT HELP?
>> IF IT'S ENCRYPTED AND THEY
ENCRYPT IT, CAN YOU DECRYPT IT
AND USE IT?
(LAUGHTER)
YOU STILL HAVE TO MAKE SURE,
EVEN IF IT'S ENCRYPTED, AND THE
ENCRYPTION HELPS WITH THE RISK
OF EXFILTRATION AND BEING ABLE
TO -- FOR THEM TO ACTUALLY BE
ABLE TO LEVERAGE THAT DATA
AGAINST YOU, BUT IF THEY ENCRYPT
YOUR ENVIPTED DATA, YOU STILL
CAN'T ACCESS IT.
>> SO, CHAD, YOU IN PARTICULAR
ARE WORKING IN THE HEALTHCARE
INDUSTRY WHICH HAS REALLY SEEN
SO MUCH OF THE RANSOMWARE,
CERTAINLY THE HIGH-PROFILE
STUFF.

I'M HOPING YOU CAN SHARE A
LITTLE BIT OF, YOU KNOW, KIND OF
WHAT IT LOOKS LIKE FROM YOUR END
AS A SECURITY PROFESSIONAL
WORKING IN HEALTHCARE THESE DAYS
AND, YOU KNOW, WHAT YOU GUYS ARE
SEEING AND TO WHAT EXTENT THAT
WHAT YOU HAVE BEEN DOING HAS
BEEN WORKING TO HELP STOP IT.
>> I'LL SUM IT UP IN ONE WORD --
IT'S SCARY.
THE NUMBER OF ATTACKS AND THE
SOPHISTICATION OF ATTACKS HAS
REALLY GROWN EXPONENTIALLY OVER
THE PAST COUPLE OF YEARS.
THERE IS NOT ONE PARTICULAR
VECTOR THAT THEY'RE USING.
THEY'RE USING MULTIPLE VECTORS
TO INFECT SYSTEMS.
THEY'RE USING MULTIPLE
TECHNIQUES TO TRICK OR SOCIAL
ENGINEER, DOCTORS,
ADMINISTRATORS, OTHER FOLKS TO

GET ON TO SYSTEMS AND ACCESS
INFORMATION.
SO IT'S SCARY.
THE CYBER HYGIENE AND PREVENTION
DOES A LOT TO ELIMINATE THE
PROBLEM RIGHT UP FRONT.
AND THEN YOU HAVE TO INVEST IN
INCIDENT RESPONSE AND
CONTAINMENT AND METHODOLOGIES
FOR MINIMIZING THE IMPACT WHEN
SOMETHING DOES HAPPEN.
SO IF YOU END UP WITH A SYSTEM
THAT -- A LAPTOP THAT GOES HOME
AND IT'S ENCRYPTED, SO IF IT'S
STOLEN OUT OF THE BACK OF A
VEHICLE OR OUT OF THE PERSON'S
POSSESSION, YOU HAVE SOME SAFE
HARBOR THERE, THE BAD GUY CAN'T
ACCESS THE DATA THAT'S ON THAT
DEVICE.
BUT IF THAT LAPTOP GOES HOME AND
THEN THAT GETS RANSOMWARE
BECAUSE IT'S ON A DIFFERENT

NETWORK, IT'S NOT ON YOUR
NETWORK, THAT DATA THAT'S ON THE
DEVICE IS EX FILTRATED, THEN YOU
STILL HAVE A LARGE ISSUE.
SO YOU HAVE TO WORK WITH THE
DIFFERENT TECHNOLOGIES, THE
DIFFERENT PARTNERS ACROSS THE
SECURITY INDUSTRY AS WELL AS
MAKING SURE THAT YOUR FOLKS THAT
ARE REALLY FOCUSED AND DOCTORS
ARE REALLY FOCUSED ON TAKING
CARE OF PATIENTS, THAT'S THEIR
PRIMARY JOB, THAT'S THE ROLE OF
OUR BUSINESS IS TO TAKE CARE OF
PEOPLE, NOW THEY HAVE TO LEARN
THAT BAD PEOPLE ARE AFTER THEM
AND THEIR INFORMATION AND THEY
NEED TO LEARN HOW TO TAKE CARE
OF THEMSELVES.
SO THAT'S EDUCATION DOES GO AA
LONG WAY. IT'S NOT THE PRIMARY
CONTROL PER SE BUT IT IS A VERY
NECESSARY CONTROL WITHIN THE

HEALTHCARE SPACE FOR PROTECTING

THE ENVIRONMENT.

>> LET ME JUST ADD TO THAT.

I THINK IT'S KIND OF INTERESTING

SORT OF CASE STUDY WHY

HEALTHCARE IS BEING TARGETED.

OBVIOUSLY, IT'S

INFORMATION-RICH, BUT IT'S ALSO

A VERY HIGH CRITICAL, HIGH

PRESSURE SITUATION.

PATIENT RECORDS, OBVIOUSLY VERY

IMPORTANT, IF THOSE GET LOCKED

UP.

PATIENT TREATMENT COULD LAPSE

AND ACTUAL LIVES ARE AT STAKE.

IT ADDS THE EXTRA PRESSURE

ELEMENT TO SUBMIT THAT

REASONSOME AND I THINK THE

PSYCHOLOGY OF THAT IS REALLY

IMPORTANT.

I THINK WE'LL SEE THAT AND MOVE

INTO OTHER CRITICAL AREAS WHERE

LIVES COULD BE AT STAKE.

>> AND ALSO WITHIN HEALTHCARE,
YOU ALSO HAVE THE FINANCIAL
ASPECT THAT YOU HAVE TO
CONSIDER.
MOST NON-PROFITS OPERATE WITH 1%
TO 3% OVERHEAD MARGIN, SO IF YOU
CAN'T ACCESS THE DATA AND YOU
CAN'T SEE THE PATIENTS TO TAKE
CARE OF THEM, IT LIKELY DRUPTS
YOUR ENTIRE FINANCIAL CHAIN OF
THE WHOLE ORGANIZATION.
SO IT GOES BACK TO THE
VIABILITY.
SECURITY IS ESSENTIALLY
IMPORTANT TO PROTECTING IN
HEALTHCARE, TO PROTECTING THE
VIABILITY OF THE BUSINESS AS
WELL, WHICH IS JUST TAKING CARE
OF PEOPLE.
THAT'S THE WHOLE FOCUS.
>> IF I COULD.
CHAD AND I WERE TALKING BEFORE
THIS ABOUT SOME OF THE

CHALLENGES IN HEALTHCARE.
WE DEAL WITH A LOT OF HEALTHCARE
ORGANIZATIONS AND MY JOB ENDS UP
BEING -- OUR STATE AND FUNCTION
IS TO DETECT THINGS BUT TO SPEND
A LOT OF TIME ADVISING CUSTOMERS
IN TERMS OF PREVENTION AND
AWARENESS.
SO THE HEALTHCARE SIDE IS
INTERESTING BECAUSE, AS YOU
MENTIONED, THERE IS A TREMENDOUS
PRESSURE TO JUST MAKE THE
PROBLEM GO AWAY BECAUSE THAT'S
NOT THE PROBLEM THAT'S GOING TO
END UP HURTING YOU OR SOMEONE
ELSE LONG TERM.
WHEN YOU TALK ABOUT PREVENTION,
PARTICULARLY FROM A CORPORATE
STANDPOINT, HEALTH CARE IS
INTERESTING IN THAT YOU'RE
STARTING TO SEE THEM RESPOND IN
THE SAME WAY THE GOVERNMENT'S
BEEN RESPONDING TO THINGS FOR A

LONG TIME, AND THESE ARE THINGS
WE HAVE BEEN PREACHING FOR
DECADES, WHICH IS ISOLATION OF
NETWORKS, REDUCTION OF
PRIVILEGE.
SO WE HAD A CUSTOMER A FEW
MONTHS AGO TO GET HIT BY A WORM.
THE THING IS RUNNING RAMPANT.
IT ONLY HAS TO GET INTO ONE
SYSTEM, STARTS RUNNING RAMPANT
ON ALL THE OTHER SYSTEMS AND
NEXT THING YOU KNOW YOU'VE GOT
PORTIONS OF A HOSPITAL INFECTED.
HOWEVER, IN THAT CASE, WHAT THE
MOST INTERESTING THING WAS IT
ENDED UP BEING -- THEY PREPARED
WELL.
SO FROM A CORPORATE STANDPOINT,
THEY HAD GOOD HYGIENE, THEY'D
TAKEN A LOT OF TIME AND PAIN AND
MADE BIG INVESTMENTS AND
PREVENTION, CONTAINMENT, NETWORK
INFRASTRUCTURE, AND, SO, WHILE

THAT ENDED UP BEING -- IN TERMS
OF SCOPE AND INFECTION -- MAYBE
THE SAME NUMBER OF SYSTEMS
INFECTED THAT YOU SEE IN OTHER
CASES THAT YOU READ ABOUT IN THE
NEWS, BUT IT ENDED UP BEING A
PROBLEM FOR THE I.T. TEAM,
PEOPLE WORKED LATE, PROBABLY
WASN'T ENJOYABLE, BUT IT DIDN'T
DISRUPT HEALTH CARE DELIVERY.
SO WHEN BUSINESSES TAKE A STEP
BACK, IDENTIFIED THE THINGS YOU
NEED TO MAKE MONEY, SAVE LIVES,
WHATEVER YOUR BUSINESS, IS AND
THEN YOU'VE GOT TO UNDERSTAND
YOUR RISK, UNDERSTAND YOUR
VICTIM PROFILE AND THEN YOU KIND
OF TAKE A STEP BACK FROM THAT
AND JUST LOOK LOGICALLY AND SAY
WHAT ARE THE REALLY SIMPLE
THINGS I CAN DO?
THEY MIGHT NOT BE CHEAP BUT
THEY'RE PROBABLY REALLY SIMPLE

TO JUST REDUCE IMPACT AND RISK
OVERALL.
SO THERE IS SO MUCH PRESSURE AND
I'M SURE WE'LL SEE IT IN OTHER
PARTS OF PUBLIC SAFETY IN THE
FUTURE.
>> SOUNDS A LITTLE FARFETCHED TO
HEAR BUT DOESN'T TAKE LONG TO
IMAGINE HOW A MOTIVATED CYBER
CRIMINAL COULD TAKE ADVANTAGE OF
OUR ENTRANCE INTO THE INTERNET
OF THINGS, I.O.T. IN PARTICULAR,
MEDICAL DEVICES, LOTS OF
VULNERABILITIES THERE, YOU KNOW,
CYBER CRIMINALS ARE ONLY SORT OF
SLOWED BY THEIR OWN IMAGINATION,
ARE ONLY LIMITED BY THEIR OWN
IMAGINATION.
SO I THINK THIS IS GOING TO
CONTINUE TO BE AN ISSUE,
ESPECIALLY IN HEALTHCARE AND IN
OTHER AREAS.
>> UNFORTUNATELY, YOU'RE

ABSOLUTELY RIGHT.

THEY'RE LIMITED BY THEIR OWN

IMAGINATION BUT IN HEALTHCARE

WE'RE LIMITED BY OUR VENDORS,

OUR PARTNERS, AND OFTENTIMES

MEDICAL DEVICE VENDORS CHARGE TO

HAVE DEVICES REIMAGED.

SO THERE IS A CHARGE TO HAVE A

TECHNICIAN COME OUT AND REIMAGE

THAT MRI CONTROLLER AND PUT IT

BACK TO F.D.A.-APPROVED

STANDARDS FOR HAVING SEEN

PATIENTS.

SO THERE IS COSTS ASSOCIATED

WITH ALL OF THAT.

SO THEY OFTEN -- WE OFTEN HAVE

TO GO THE EXTRA MILE TO GET

INFORMATION FROM A PROVIDER

PERSPECTIVE TO GET INFORMATION

FROM OUR MEDICAL DEVICE

MANUFACTURERS AROUND PROTECTING

THOSE DEVICES AND WHAT WE CAN

AND CANNOT DO.

IN THE PAST, HISTORICALLY, UP TO
TWO TO THREE YEARS AGO, WE WERE
VERY HAMSTRUNG FROM MEDICAL
DEVICE MANUFACTURERS NOT REALLY
PROVIDING UP-FRONT CONTROLS TO
BE PUT IN PLACE FOR THOSE
DEVICES TO PROTECT THEM.
YEAH.
>> WE HAD TO GO ASK VERY
SPECIFIC QUESTIONS.
WHAT DOES THAT MODALITY NEED TO
DO TO TALK TO THE JOB WITHIN THE
HOSPITAL.
WHAT OTHER MODALITIES DOES IT
NEED TO TALK TO?
WHEN I PUT I FIRE WALL HERE,
DOES THAT STOP THE DEVICE FROM
FUNCTIONING?
WE HAVE TO ASK THOSE QUESTIONS
ON A REGULAR BASIS AND REALLY
SEGMENT OUR NETWORKS, GOING BACK
TO HYGIENE 101, IS IF THE
DEVICES DON'T NEED TO TALK TO

EACH OTHER FOR BUSINESS, THEN
WHY DO WE ALLOW IT.
A LOT OF TIMES IT'S JUST BECAUSE
IT'S BEEN CONVENIENT.
IT'S EASIER TO PUT SOMETHING IN
PLACE AND CONNECT ID TO A
NETWORK LIKE WE DO AT HOME AND
LET THINGS TALK TO EACH OTHER
VERSUS ACTUALLY PUTTING THAT
SEGMENTATION IN PLACE AND
LIMITING COMMUNICATION.
>> IF YOU'RE SOMEONE OUT THERE
LISTENING TO THE WEBCAST WHO IS
WORRIED ABOUT RANSOMWARE AND
REALIZING THEY HAVEN'T DONE SOME
OF THESE THINGS, WHERE DO YOU
START?
IS THERE A GOOD STARTING PLACE
TO BEGIN BUILDING OUT A PROGRAM?
>> FOR A CONSUMER OR HEALTH
CARE?
>> MAYBE NOT SPECIFICALLY TO
HEALTH CARE, BUT FOR A BUSINESS,

LET'S SAY.

YOU KNOW, SOMEBODY WHO'S HOLDING

PERSONAL INFORMATION AND WHO'S

LOOKING TO MAKE THEIR NETWORKS

MORE SECURE?

>> FROM MY PERSPECTIVE, THERE'S

A LOT OF MATERIAL OUT THERE.

YOU HAVE SANDS, YOU HAVE NIST,

YOU HAVE YOUR DIFFERENT VENDORS

AND PARTNERS YOU CAN WORK WITH.

I DON'T WANT TO NAME THEM ALL.

SOME OF THEM ARE SITTING HERE.

>> I WOULD BE HAPPY TO NAME

THEM.

>> SOME OF THEM ARE SITTING IN

THE ROOM, SOME OF THEM ARE

LISTENING.

BUT THERE IS A LOT OF MATERIAL

ABOUT WHERE TO START.

THE WAY THAT WE APPROACHED IT AT

CHILDREN'S WAS VISIBILITY AS

WELL AS THE FOUR LIFE SAVING

STEPS FROM THE RED CROSS -- STOP

THE BLEEDING, START THE

BREATHING, PROTECT THE WOUND AND

TREAT FOR SHOCK.

WHEN YOU STOP THE BLEEDING YOU

MAKE SURE YOU KNOW WHAT ASSETS

ARE THERE.

WHERE ARE YOU HEMORRHAGING AND

WHAT DATA IS LEAVING THE

ORGANIZATION YOU'RE NOT AWARE

OF.

TAKE A LOOK AND SEE WHAT'S

HAPPENING IN YOUR ENVIRONMENT.

THEN MOVE FORWARD FROM THERE.

TURN OFF KNOWN BAD.

THERE IS PLENTY OF LISTS YOU CAN

GET FROM CYBER INTELLIGENCE

VENDORS, WE HEARD FROM CISCO AND

THE TALOS INTELLIGENCE GROUP.

WE USE THEM AND OTHER FOLKS AS

WELL.

TURN OFF KNOWN BAD.

THERE IS REALLY NO REASON YOU

HAVE TO GO TO A MALWARE INFECTED

SITE THAT IS KNOWN TO BE

INFECTED, AND SECURITY

INTELLIGENCE COMMUNITIES KNOW

THEY'RE INFECTED.

YOU HAVE TO LEVERAGE THAT

INFORMATION.

IF IT IMPACTS THE BUSINESS, MAKE

FOLKS PUT THEIR HAND IN THE AIR

AND SAY, HEY, THIS IS AN IMPACT

AND GO THROUGH AN EXCEPTION AND

A VETTING PROCESS.

IT WORKS IN HEALTH CARE.

THERE IS PROVIDER ORGANIZATIONS

THAT DON'T DO THAT AND THEY'VE

GOTTEN HIT.

THERE IS OTHER ORGANIZATIONS

THAT ARE JUST STARTING TO DO

THAT IN THE HEALTH CARE

BUSINESS, BUT WE SHOULD BE DOING

THAT AS CONSUMERS EVERYDAY AT

HOME AND THINKING ABOUT WHAT ARE

WE CONNECTING TO, WHAT ARE WE

CLICKING ON.

>> I DID GET A NOTE FROM OUR
I.T. PEOPLE TO REMIND PEOPLE TO
PLEASE SPEAK DIRECTLY INTO THE
MICS AS WE GO ON.
SO, LORRIE, ONE OF THE THINGS I
WAS HOPING TO DISCUSS WITH YOU,
AND WE'VE TALKED A BIT ABOUT
AWARENESS IS A BIG PROBLEM, AND
THAT THE HUMAN ELEMENT,
CERTAINLY FOR THE EMAIL VECTOR,
IS PROBABLY GOING TO BE THE
WEAKEST LINK OF THE SECURITY
CHAIN.
THIS IS AN AREA THE COMMISSION
AND ELSEWHERE HAS WORKED ON
TRYING TO EDUCATE PEOPLE FOR
YEARS NOW.
WHAT ARE THE BIGGEST CHALLENGES
IN TERMS OF TRAINING AND ARE
THERE ANY TECHNIQUES OUT THERE
THAT ARE LIKELY TO BE MORE
EFFECTIVE?
>> AT CARNEGIE MELLON WORKING

WITH MY STUDENTS THERE, WE'VE
ACTUALLY DONE A LOT OF RESEARCH
ON WHAT IS EFFECTIVE, AND THERE
ARE SOME TECHNIQUES THAT WORK.
I KNOW WE SAID EARLIER THIS
MORNING, YOU CAN'T TELL PEOPLE
NOT TO CLICK ON LINKS, AND YET
LINKS ARE MEANT TO CLICK ON, SO
IT IS A DIFFICULT CHALLENGE.
BUT THERE ARE SOME THINGS THAT
YOU CAN DO TO HELP PEOPLE JUDGE
LINKS BETTER.
WHAT WE DID IN OUR RESEARCH IS
WE WATCHED EXPERTS CLICK ON
LINKS.
WE LOOKED TO SEE WHAT WERE
EXPERTS DOING WHEN THEY WERE
MAKING THESE JUDGMENTS AND WHAT
IS IT THAT EXPERTS ARE DOING
THAT WE MIGHT BE ABLE TO TEACH
TO PEOPLE WITHOUT HAVING TO
TEACH THEM EVERYTHING AN EXPERT
ALREADY KNOWS.

SO AN EXAMPLE OF THE KEY THING
THAT WE FOUND IS EXPERTS TEND TO
LOOK AT THE URLs, AND THEY'RE
MAKING A JUDGMENT BASED ON WHAT
THEY SEE IN THAT URL BECAUSE
THEY UNDERSTAND THE COMPONENTS
OF THE URL AND WHAT SHOULD BE
THERE AND WHETHER TO KNOW THAT'S
THE URL YOU WOULD EXPECT TO HAVE
IN THAT SITUATION.
SO WE FOCUSED ON CAN WE TEACH
CONSUMERS THAT.
MY STUDENTS DEVELOPED A LITTLE
VIDEO GAME TO TEACH PEOPLE HOW
TO UNDERSTAND URLs, AND WE DID
RESEARCH STUDIES AND FOUND THAT
WAS ACTUALLY FAIRLY EFFECTIVE.
DID IT PREVENT PEOPLE FROM EVER
CLICKING ON A BAD LINK?
NO, BUT IT SUBSTANTIALLY REDUCED
THE NUMBER OF BAD LINKS THAT
THEY CLICKED ON.
SO IT'S TECHNIQUES LIKE THAT

THAT I THINK CAN BE EFFECTIVE IN
EDUCATING PEOPLE AND REDUCING
THEIR VULNERABILITY.
>> AND WHEN YOU LAYER THOSE
TECHNIQUES ALONG WITH OTHER
TECHNOLOGY, LIKE DO YOU NEED TO
HAVE ACTIVE CONTENT IN YOUR
EMAIL?
DO YOU NEED TO PRESENT THEM WITH
LINKS TO CLICK ON?
THOSE KIND OF QUESTIONS SEEM
PRETTY BASIC, BUT NOT A LOT OF
EMAIL NEEDS ACTIVE LINKS.
TAKE THAT AN EXTRA MILE, WE
INVESTED IN PREVENTION THAT
LOOKS AT OUR THOSE LINKS WITHIN
AN EMAIL, AND WE WERE ABLE TO
REMOVE WELL OVER TWO-THIRDS OF
THOSE LINKS BECAUSE THEY WERE
KNOWN MALWARE, THEY WERE KNOWN
BAD.
THE SECURITY INTELLIGENCE
COMMUNITY KNEW THOSE LINKS WERE

BAD AND WE WERE JUST ABLE TO NOT
DELIVER THOSE E-MAILS.
SO THERE IS A LOT YOU CAN DO IN
ADDITION TO THE EDUCATION FOR
FOLKS TO REMOVE THE RISK OF
POTENTIALLY CLICKING ON A BAD
LINK, IF YOU MAKE THE DECISION
THAT YOU WANT TO DELIVER LINKS
TO THE END USER.
>> ANYTHING THAT YOU CAN
AUTOMATE OUT IS GOING TO NOT
ONLY MAKE PEOPLE SAFER BUT
REDUCE THE BURDEN ON THE END
USER, AND END USERS DON'T WANT
TO HAVE TO SPEND ALL THEIR TIME
DOING SECURITY, THAT'S NOT WHY
THEY USE THEIR COMPUTERS.
SO WE'RE SEEING COMPANIES DOING
THAT.
EVEN THE LARGER EMAIL PROVIDERS
DO THAT WHERE THEY HAVE LISTS OF
KNOWN MALWARE AND PHISHING SITES
AND THEY'RE ALSO FILTERING THOSE

THINGS OUT.

>> THIS WILL BE BUSINESS

SPECIFIC AND NOT CONSUMER

SPECIFIC BUT, YEAH, THERE ARE.

I THINK WE'VE ALREADY TALKED

AROUND IT OR ABOUT IT DIRECTLY.

YOU'VE MENTIONED THE THINGS

EXPERTS DO -- THEY LOOK

CAREFULLY AT THE LINK, MAKE SURE

IT DOESN'T JUST SAY THE WORD

THEY EXPECTED, THEY LOOK BEHIND

IT, HOVER OVER IT AND MAKE SURE

IT'S THE WEB SITE YOU EXPECTED.

SO THAT SERVICE, THERE IS PLENTY

OF PROVIDERS, A GREAT T-UP FOR

BILL SO, THERE IS PLENTY OF

PLACES.

DO WHAT THE EXPERTS DO AND

AUTOMATE IT.

YOU CAN BUY IT.

LET SOMEONE WHO HAS A TEAM OF

PEOPLE LOOK AT EVERY LINK FOR

YOU AND AS A BUSINESS THE LINKS

YOU GET WILL NEVER BE A LINK

DIRECTLY TO THE WEB SITE.

THE EMAIL COMES IN, TAKE THE

LINKS OUT, STRIP OUT THE BAD

ONES, THEY SANITIZE THINGS AND

YOU PASS THAT TRAFFIC THROUGH

EVERYTHING.

SO YOU EFFECTIVELY HAVE SOMEONE

LOOKING AT YOUR INBOUNDS.

THE TRAINING SIDE, SERVICES WILL

SEND THE PHISHING E-MAILS

PERIODICALLY TO YOUR EMPLOYEES.

THEY WILL MEASURE SUCCESS RATE

FOR THOSE THINGS AND IF THE

EMPLOYEES FAIL THE TEST THEY GET

ON THE SPOT TRAINING.

SO THERE IS A NUMBER OF

TECHNIQUES.

>> THE SECURITY SOFTWARE OUT

THERE NOW IS NOT JUST LIKING AT

KNOWN LINKS OR KNOWN FILES, IT'S

LOOKING AT THE BEHAVIOR -- WHERE

HAVE WE SEEN THIS ON THE WEB

BEFORE -- SO WE'RE GETTING VERY
GOOD AT DETECTING BAD FILES AND
BAD LINKS.
>> SO ON THE RANSOMWARE-SPECIFIC
FRONT, WE'VE HEARD TALK ABOUT
THINGS LIKE DESCRIPTION KEYS OR
VACCINES FOR RANSOMWARE.
TO WHAT EXTENT HAVE YOU SEEN
THIS OUT IN THE WILD AND IS THAT
SOMETHING PEOPLE CAN REASONABLY
RELY ON IN TERMS OF GETTING
THEIR INFORMATION BACK IS THIS.
>> YOU KNOW, OCCASIONALLY, I
SUPPOSE THERE IS AN INCOMPETENT
RANSOMWARE ACTOR WILL INCLUDE A
DESCRIPTION KEY IN THEIR PAY
LOAD OR USE THE SAME KEY ON
SEVERAL VICTIMS, SO THIS WOULD
ALLOW ANYONE WITH A CERTAIN
LEVEL OF TECHNOLOGICAL EXPERTISE
TO DECRYPT THEIR FILES.
UNFORTUNATELY THOSE MISTAKES
ARE, A, FEW AND FAR BETWEEN AND

THEY ARE QUICKLY COVERED, SO I
WOULD NOT RELY ON THAT AT ALL.
THERE IS ONLY A SMALL NUMBER OF
VICTIMS OUT THERE AND COULD
REALLY EVER TAKE ADVANTAGE OF
THAT, IS MY VIEW.
>> AND YOU KEEP HEARING THE WORD
SASS, YOU'RE DEALING WITH
SOFTWARE AS A SERVICE.
IT'S SHARED, SO THE HALF-LIFE OF
BUGS, IF GOOGLE PUSHES OUT A BAD
CODE RELEASE, EVERYONE WILL
NOTICE IT, CONVERGE ON IT FAST
AND FIX IT.
YOU HAVE A HALF-LIFE IN BUGS IN
GOOD SOFTWARE AND YOU HAVE THE
SAME THING.
SO I WOULD NEVER RELY ON IT.
IT MIGHT SAVE YOU IN A PINCH IF
YOU'RE REALLY LUCKY, BUT IT'S
DEFINITELY NOT SOMETHING YOU
WANT TO HANG YOUR HAT ON, I
DON'T THINK.

>> ANY OTHER IDEAS ABOUT WHY
RANSOMWARE HAS BEEN SO HARD TO
STOP OR WHY LAW ENFORCEMENT IN
PARTICULAR HASN'T BEEN ABLE TO
FINGER THESE GUYS AND PUT AN END
TO IT?
>> YOU KNOW, I THINK THE GROWTH
HAS BEEN UNDENIABLE.
I THINK LAST YEAR THERE WERE 100
NEW FAMILIES OF RANSOMWARE, IT'S
AN ALL-TIME HIGH.
A LOT OF IT IS, AGAIN, SUCCESS
IS BREEDING SUCCESS.
THEY HAVE REFINED -- THE BAD
GUYS HAVE SORT OF REFINED THEIR
BUSINESS MODEL.
THEY'VE FOUND JUST THE RIGHT
AVERAGE RANSOM AMOUNT THEY KNOW
THEY CAN ASK FOR AND STILL
POSSIBLY GET THEIR MONEY BACK.
LAST YEAR, OR 2014, ROUGHLY
$300.
THIS YEAR HOPPED UP TO $700.

THAT SEEMS TO BE THE EQUILIBRIUM
THERE.
AND THE WIDE-SCALE DISCRIMINATE
STUFF GOES ON, IT'S GETTING MORE
AND MORE TARGETED TO THE
ORGANIZATION.
SO WITH RESPECT TO SORT OF LAW
ENFORCEMENT INVOLVEMENT, AND
IT'S EXTREMELY DIFFICULT TO
TRACK THIS DOWN, THE F.B.I. HAS
A HELL OF A LOT GOING ON RIGHT
NOW, PROBABLY OUTSIDE OF
RANSOMWARE.
SO I THINK, IN MANY WAYS, IT'S
SORT OF UP TO US TO PROTECT
OURSELVES.
>> SO ONE QUESTION THAT WE'VE
GOTTEN FROM THE AUDIENCE IS
ABOUT MOBILE RANSOMWARE, IN
PARTICULAR.
AND, YOU KNOW, TO WHAT EXTENT AS
A CONSUMER, IF YOU HAVEN'T JAIL
BROKEN YOUR PHONE, IF YOU'RE NOT

GOING TO THIRD PARTY APP STORES
AND YOU'RE RELYING ON PRETTY
REASONABLE SOURCES, IS THAT THE
KIND OF THING THAT'S GOING TO
MAKE YOU SECURE ON YOUR MOBILE
PHONE?
DO YOU STILL NEED TO WORRY ABOUT
RANSOMWARE?
>> YEAH, YOU SHOULD ALWAYS BE
WORRIED.
YEAH, I MEAN, I THINK IT HELPS
TO GO TO THE MAJOR APP STORES,
BUT EVEN THERE, THERE CAN STILL
BE SOME BAD APPS.
AND, SO, I THINK, YOU KNOW, KIND
OF THE MOST STRAIGHTFORWARD
THING THAT A CONSUMER CAN DO
WHEN THEY GO TO DOWNLOAD AN APP
IS TO SEE DOES THIS LOOK LIKE A
POPULAR APP THAT'S BEEN HERE A
WHILE, OR IS THIS SOMETHING THAT
MIGHT HAVE A NAME THAT SOUNDS
SIMILAR TO SOMETHING YOU KNOW OR

IT JUST POPPED UP HERE A FEW
HOURS AGO, HASN'T BEEN
DOWNLOADED VERY MUCH.
MAKE SURE YOU'RE DOWNLOADING
WHAT YOU THINK YOU'RE
DOWNLOADING.
>> SO THE SAME FUNDAMENTAL
PROBLEM AT THE YOU RUN INTO WITH
COMPUTERS, RIGHT.
SO SECURITY, I THINK WHAT WE'VE
HEARD PRETTY MUCH ALL DAY IS
THERE IS A BIG SERIES OF
TRADEOFFS YOU HAVE TO MAKE,
BEING A SECURITY MANAGER OR
DIRECTOR AND NOW IT'S BEING A
CONSUMER.
SO I THINK THE SAME -- IF YOU
PRACTICE SOME OF THESE BASIC --
GET INTO REALLY BASIC HABITS, SO
IF YOU'RE ON A COMPUTER, AGAIN,
IF YOU CAN OPEN YOUR COMPUTER,
GET TO YOUR BACKUPS, SO CAN THE
MALWARE.

SAME THING IS TRUE OF YOUR

PHONE.

ALL THE MAJOR SMARTPHONE

PROVIDERS HAVE A BUILT-IN BACKUP

MECHANISM.

UNDERSTAND WHERE THOSE FILES GO.

TAKE A MINUTE TO UNDERSTAND HOW

TO GET TO THEM.

IF THERE ARE THINGS YOU REALLY

CARE ABOUT OR IF THEY'RE THE

ONLY PICTURES YOU HAVE IN THE

WORLD OF YOUR KIDS, TAKE TIME TO

GET THOSE OUT OF THERE, IF YOU

CAN, PUT THEM ON A DISK, STUFF

THE DISK IN A DRAWER.

AGAIN, SAME THING THAT YOU DO

FOR A COMPUTER, FOR AN iPad,

FOR A PHONE.

YOU KNOW, YOU TRADE A LITTLE BIT

OF CONVENIENCE AND YOU'RE GOING

TO HAVE TO SET A REMINDER AND

PLUG THE THING IN, BUT IF YOU

TRADE A LITTLE BIT OF

CONVENIENCE, YOU GET A LOT IN

RETURN.

IT APPLIES TO PRETTY MUCH ANY

DEVICE PROFILE.

>> I SEE WE ARE ALMOST OUT OF

TIME.

SO I'LL ASK IF THERE IS ANY

FINAL THOUGHTS FROM THE GROUP.

I DON'T BELIEVE WE HAVE ANY

OTHER QUESTIONS FROM THE

AUDIENCE.

BUT IF NOT, I THINK WE WILL WRAP

UP NOW.

SO THANK YOU VERY MUCH FOR YOUR

TIME.

>> THANK YOU.

WE REALLY APPRECIATE IT.

(APPLAUSE)

;;;;Panel 3

UP NEXT I'LL BRING UP WILL MAXON

FROM DIVISION OF MARKETING

PRACTICES WHO WILL INTRODUCE OUR

THIRD PANEL.

>> THANKS VERY MUCH FOR STICKING

AROUND TO THE FINAL PANEL.

REALLY APPRECIATE EVERYONE

COMING AND ALL OF OUR PANELISTS

THAT WE HAVE HERE.

FOR THE THIRD PANEL, WE'LL TALK

ABOUT WHAT TO DO IF YOU GET HIT

BY RANSOMWARE, IF YOU'RE

INFECTED WITH RANSOMWARE.

I THINK AS GEORGIA MENTIONED

THIS MORNING, ETCH THE MOST

SOPHISTICATED I.T. PEOPLE

SOMETIMES BYPASS BEST SECURITY

PRACTICES AND DO THINGS THAT YOU

SHOULDN'T BE DOING ON THE

INTERNET, CLICKING ON LINKS YOU

DON'T KNOW OR INSTALLING

SOFTWARE YOU'RE NOT SURE ABOUT,

SO YOU COULD GET HIT, AND WE'RE

GOING TO TALK ABOUT WHAT TO DO

IF YOU ARE.

OUR PANELISTS ARE A GREAT

COLLECTION OF PEOPLE WHO ARE
HERE TO TELL YOU EXACTLY WHAT WE
CAN DO IF YOU'RE HIT.
FIRST OF ALL, ON THE FAR END,
WITHOUT A NAME TAG,
UNFORTUNATELY, IS WILL BALES, A
SUPERVISORLY SPECIAL AGENT IN
THE CYBER DIVISION OF THE
FEDERAL BUREAU OF INVESTIGATION.
HE'S CURRENTLY ASSIGNED TO THE
MAJOR CYBER CRIMES UNIT, CYBER
DIVISION WHERE HE IS RESPONSIBLE
OF LEADING THE F.B.I.AS EFFORT
AGAINST RANSOMWARE.
NEXT TO WILL, WE HAVE PAAÄIVI
TYNNINEN.
PAAÄIVI IS A RESEARCHER AT
F-SECURE AND FOCUSES ON
MONITORING THE THREAT LANDSCAPE
BY DOING THREAT INTELLIGENCE,
MALWARE, ANALYSIS AND REVERSE
ENGINEERING.
HER EXPERTISE IS FOLLOWING

BOTNETS, RANSOMWARE.

SERGE JORGENSEN, PRESIDENT OF

THE SYLINT GROUP, PROVIDES

RESPONSIVE MEDIATION GUIDANCE TO

MT. BILLION DOLLARS ESPIONAGE

AND CYBER SECURITY ATTACKS.

WE HAVE ADAM MALONE, DIRECTOR OF

CYBER INVESTIGATIONS AND BREECH

RESPONSE PWC.

RIGHT NEXT TO ME WE HAVE BILL

HARDEN, VICE PRESIDENT OF

CHARLES RIVER ASSOCIATES.

WORKED ON DATA BREECH AND

CYBERINCIDENT RESPONSE, THEFT OF

TRADE SECRETS, WHITE-COLLAR

CRIME AND ENTERPRISE RISK

MANAGEMENT.

FIRST OF ALL, THANK YOU SO MUCH

FOR BEING HERE.

WE REALLY APPRECIATE IT.

THE FIRST QUESTION I'M GOING TO

POSE IS WHAT IS THE FIRST THING

THAT A CONSUMER OR SMALL

BUSINESS SHOULD DO IF THEY'RE
INFECTED BY RANSOMWARE, IF THEY
GOAT ONE OF THOSE POP-UPS WE SAW
EARLIER WITH A SKULL AND
CROSSBONES OR WHATEVER SAYING
ALL YOUR FILES ARE ENCRYPTED,
YOU NEED TO PAY US X NUMBER OF
BITCOINS.
BILL, COULD YOU LEAD US OFF?
>> SURE.
SO CHARLES RIVER, WE LIKE TO DO
WHAT I CALL THE ACRONYM BEING
CPA.
SO WHAT DOES THAT MEAN?
WELL, FIRST OFTEN, WE WANT TO
CONTAIN THE EVENT OF WHAT'S
HAPPENED, CONTAINMENT MEANS THE
SKULL AND CROSSBONES HAVE NOW
COME UP, WHO DO I NEED TO CALL?
DO I NEED TO CALL SOMEONE WITH
AN I.T. WITHIN MY ORGANIZATION,
HEY, I ACCIDENTALLY JUST DID
THIS, CAN YOU GUYS HELP ME OUT.

THE NEXT PART OF THAT IS GOING
TO BE PRESERVATION IN OUR CPR
ANALOGY.
PRESERVATION.
BEING A FORENSIC INVESTIGATOR,
WE HAVE TO PRESERVE EVIDENCE
BECAUSE WHEN WE COME ON THE
SCENE, WE NEED TO UNDERSTAND
EXACTLY WHAT HAPPENED.
LASTLY, WILL, THE THING THAT WE
NEED TO TALK ABOUT IS
REMEDIATION.
THAT'S SOMETHING HERE THAT THE
PANEL IS GOING TO TALK ABOUT.
PAY OR NOT PAY?
I KNOW A LOT OF PEOPLE HAVE
TALKED ABOUT THE ASPECT OF WE
HAVE THE BACKUPS.
BUT NOW LET'S SAY WE DON'T HAVE
THE BACKUPS, FROM A BUSINESS
PERSPECTIVE, ARE WE GOING TO
MAKE A PAYMENT?
IF WE DO, HOW DO WE SET UP A

BITCOIN WALLET?

HOW IS IT GOING TO WORK?

WITH THAT, WILL, I GO WITH THE

CPR WHEN I TALK TO CLIENTS, I

THINK IT HELPS OUT AND CALMS

THEM DOWN A LITTLE BIT.

>> SO LET'S SAY YOU'RE HIT NOW

AND TRYING TO ANALYZE WHAT

YOU'RE GOING TO DO, THE FIRST

THING I THINK A LOT OF PEOPLE

WILL THINK OF IS SHOULD I REPORT

THIS TO LAW ENFORCEMENT, AND IF

I DO REPORT IT TO LAW

ENFORCEMENT WHO AM I SUPPOSED TO

CONTACT?

IS IT LOCAL, STATE, FEDERAL?

AND IF SO, WHAT KIND OF RESPONSE

SHOULD I EXPECT FROM LAW

ENFORCEMENT?

AND I THINK, WILL, YOU'RE THE

NATURAL PERSON TO RESPOND TO

THAT FIRST.

>> SURE.

I WOULD SAY YOU SHOULD
DEFINITELY REPORT IT TO LAW
ENFORCEMENT.
THE F.B.I. HAS BEEN TAKING THE
LEAD ON ANY TYPE OF RANSOMWARE
EVENT OR INCIDENT, AND WITH
THAT, WHAT YOU ARE TO EXPECT
FROM THE F.B.I., I DO NOT WANT
TO GUARANTEE THAT YOU WILL HAVE
A WHOLE BUNCH OF F.B.I. AGENTS
SHOW UP AT YOUR DOOR.
I JUST CAN'T PROMISE THAT.
IT'S PROBABLY A GOOD THING FOR
MANY OF YOU.
HOWEVER, WE DO AND ARE VERY
SYMPATHETIC TO THE IMPACT IT IS
CAUSING YOU, WHETHER AT A
PERSONAL LEVEL, BUSINESS,
CORPORATION, HEALTHCARE
PROVIDER, WE ARE VERY
SYMPATHETIC.
WHEN YOU CALL AND REPORT TO LAW
ENFORCEMENT, WE CAN TAKE THE

INFORMATION YOU OBTAINED,
WHETHER THE BITCOIN WALLET OR
ANY TYPE OF TRANSACTION DATA
THAT MIGHT BE OCCURRING, ANY
TYPE OF EPAIL ACCORDANCE THAT
YOU MIGHT BE HAVING WITH THE
SUBJECT, WE'RE VERY INTERESTED
IN THAT INFORMATION.
THAT WILL BE ABLE TO BENEFIT
BECAUSE, AS YOU ARE WELL AWARE
NOW, RANSOMWARE IS NOT AFFECTING
JUST ONE PERSON OR ONE BUSINESS,
IT'S GOING TO MOVE ON, OR
PROBABLY SIMULTANEOUSLY
AFFECTING SOMEBODY ELSE.
SO THE INFORMATION THAT YOU CAN
REPORT TO THE F.B.I. IS HUGE AND
CAN BE ABLE TO BE GATHERED SO
THAT WE CAN ADVANCE OUR
INVESTIGATION, AND I KNOW THAT
IT WAS BROUGHT UP LAST PANEL
DISCUSSION.
THESE ARE DIFFICULT

INVESTIGATIONS.

THEY ARE EXTREMELY DIFFICULT.

THE ONLY WAY WE CAN REALLY MOVE

FORWARD IS WITH THE HELP THAT

WAS BROUGHT UP.

INFORMATION FROM VICTIMS OR

ANYBODY THAT MIGHT BE ASSISTING

WITH A RANSOMWARE INCIDENT IS

GOING TO FURTHER OUR

INVESTIGATION.

SO I HIGHLY ENCOURAGE, IF YOU

ARE VICTIM TO A RANSOMWARE

EVENT, PLEASE REPORT IT TO YOUR

LOCAL F.B.I. OFFICE, OR YOU CAN

REPORT IT TO IC3.gov.

I KNOW IT'S SOMETIMES AN

INCONVENIENCE TO PICK UP THE

PHONE AND CALL.

WE DON'T IDENTIFY OURSELVES AND

YOU'RE TALKING WITH AN F.B.I.

AGENT AND STUFF, BUT IF YOU WANT

TO GO ON THE WEB SITE IC3.gov,

FILL OUT A FORM, PUT ANY

INFORMATION YOU CAN INTO THE
FORM, THEN WE'LL BE ABLE TO GET
THE INTEL FROM YOU AND BE ABLE
TO ASSIST WITH OUR CASES.
>> SPEAKING OF THE CASES THAT
THE F.B.I. BRINGS, I KNOW WE
HAVE THE ISSUE AT THE F.T.C.
WITH SOME OF OUR INTERNATIONAL
AND CROSS-BORDER ENFORCEMENT, IS
THERE MUCH THE F.B.I. CAN DO ON
THE LAW ENFORCEMENT SIDE WHEN
THE SUSPICION WOULD BE PROBABLY
IN MANY OF THESE CASES THAT THE
BAD PEOPLE ARE OUTSIDE OF THE
UNITED STATES?
>> ABSOLUTELY.
WE HAVE EXCELLENT RELATIONSHIPS
WITH WITH A LOT OF FOREIGN
PARTNERS.
WE HAVE NOT AS EXCELLENT
RELATIONSHIPS WITH SOME FOREIGN
PARTNERS.
HOWEVER, RANSOMWARE IS HIT HING

EVERYBODY, AS A WHOLE.

IT'S A GLOBAL PROBLEM.

THE VARIANT THAT THE UNITED

STATES IS BEING AFFECTED BY IS

ALSO AFFECTING NUMEROUS OTHER

COUNTRIES.

SO WE HAVE A LOT OVERJOINT

INVESTIGATIONS THAT WE CAN PASS

INFORMATION AND FURTHER BOTH OF

OUR CASES ALONG, AND WE DON'T

CARE IF THE SUBJECT IS LOCATED

IN THE UNITED STATES.

WE'LL WORK WITH OUR FOREIGN

COUNTERPARTS AND ARREST THEM IF

WE CAN.

>> IF I COULD ADD ON TO THAT, I

THINK YOU ARE TOUCHING ON SOME

OF THE ISSUES AS FAR AS

INTERACTING WITH LAW

ENFORCEMENT, BUT WE GET A LOT OF

QUESTIONS FROM CLIENTS THAT ARE

A LITTLE BIT LEERY ABOUT

REACHING OUT TO LAW ENFORCEMENT.

THEY DON'T WANT EITHER THE
PUBLICITY OR THE INTERACTION,
AND THEIR LAWYERS OR LEGAL
COUNSEL MIGHT BE COUNSELING
THEM, IF YOU DON'T WANT TO,
DON'T MAKE THE CALL.
BUT A COUPLE OF PIECES OF
INFORMATION, THE BITCOIN WALLET
ADDRESS YOU HAVE BEEN ASKED TO
PAY TO IS A GOOD PIECE OF
INFORMATION AND THE MALWARE
SAMPLES AND MASH OF THE MALWARE
CAN REALLY HELP WITH THE ONGOING
LAW ENFORCEMENT INVESTIGATIONS
AND DOESN'T NECESSARILY REVEAL
ANY INFORMATION ABOUT THE PERSON
THAT WAS ATTACKED.
SO YOU COULD MAKE AN ANONYMOUS
CALL OR GET YOUR LAWYER TO DO IT
FOR YOU AND SAY, HEY, THE CLIENT
HAD A PROBLEM, HERE'S THE TWO
BITS OF INFORMATION AND IT WOULD
STILL PROVIDE ASSISTANCE TO YOU

IN YOUR INVESTIGATION AND NOT
NECESSARILY CAUSE ALL THAT
QUANDARY ABOUT DO I REACH OUT TO
LAW ENFORCEMENT OR NOT.
>> ABSOLUTELY.
I APPRECIATE THAT.
LIKE YOU SAID, THE BITCOIN
WALLET AS WELL AS THE MALWARE
SAMPLE, EVEN JUST THE HASH VALUE
OF THAT, WE CAN GO ON OUR WAY.
OUR PURPOSE IS TO TRACK DOWN BAD
GUYS.
THAT'S WHAT WE DO IN LAW
ENFORCEMENT.
IT'S NOT A MEDIA GAME.
WE DON'T WANT ANY TYPE OF
PUBLICITY RELATING TO ANY RRMDZ
INCIDENT, THAT ONLY USUALLY
MAKES OUR INVESTIGATIONS MORE
DIFFICULT.
SO WE DO NOT MIND ANY TYPE OF
SUBMITTING OF ANONYMOUS
INFORMATION LIKE THAT.

IF YOU CAN JUST PROVIDE THAT IN
SOME WAY, THAT WOULD BE VERY,
VERY BENEFICIAL.
>> SO LET'S SAY YOU'VE GOTTEN
HIT WITH RANSOMWARE AND YOU
STARTED YOUR INITIAL RESPONSE TO
THAT INCIDENT, WHETHER IT'S AN
INDIVIDUAL OR SMALL BUSINESS,
YOU CONTACTED LAW ENFORCEMENT,
REPORTED IT, YOU'VE TURNED OFF
YOUR COMPUTER, WHATEVER ELSE IT
IS YOU'RE GOING TO DO.
I KNOW THIS IS TOUCHED ON A
LITTLE BIT IN THE HAST PANEL,
BUT IF YOU HAVE FILES IN THE
CLOUD, LIKE DROPBOX OR ICLOUD,
IS THERE ANYTHING YOU COULD DO
AT THAT POINT TO PROTECT THOSE
FILES OR WALL THEM OFF OR ARE
THOSE LOST?
SERGE, COULD YOU START US OFF?
>> SURE.
ONE OF THE THINGS, AND YOU

TOUCHED ON IT BRIEFLY, THE FIRST
CONTAINMENT PIECE, BILL, WAS
REALLY TO MAKE SURE THAT THE
COMPUTER THAT WAS DOING THE
ENCRYPTING, THE COMPUTER THAT
HAD BEEN INFECTED WAS NO LONGER
ABLE TO ENCRYPT THOSE FILES, SO
IT'S UNPLUGGING IT FROM YOUR
NETWORK JACK, TURNING OFF
WIRELESS AND SOMEHOW TRYING TO
DISRUPT THE CONNECTION THAT IT
MIGHT HAVE TO THOSE CLOUD
REPOSITORIES.
SO THE DROPBOX AGENT THAT'S
SITTING ON YOUR COMPUTER, FOR
INSTANCE, ALLOWS THE RANSOMWARE
ON YOUR COMPUTER TO ACCESS THE
FILES AND DROP BOX JUST LIKE IT
WAS A LOCAL FILE SHARE.
SO THE RAINSUM WILL START
ENCRYPTING IT.
IF YOU CAN SHUT DOWN THE AGENT
OR DISCONNECT WIRELESS AND

DISCONNECT YOUR NETWORK CABLE

AND STOP THAT CONNECTIVITY.

WE'VE SEEN MALWARE AND

RANSOMWARE TARGETING DROPBOX,

ONE DRIVE, ICLOUD, THE CLOUD

REPOSITORIES, AND THE FASTEST

THING TO DO IS TO BREAK THAT

CONNECTION.

A LOT OF TIMES WE'VE SEEN THE

CLOUD SERVICE PROVIDERS COULD

START DETECTING THE ENCRYPTED

FILES AS MALWARE AND COULD START

DELETING THEM OR THEY MAY

RECEIVER THE CONNECTION FOR YOU

AND SEND COMMUNICATION TO YOU

SAYING, HEY, WE THINK THERE IS A

PROBLEM WITH YOUR ACCOUNT, WE'VE

CUT THAT CONNECTION.

SO THE CLOUD PROVIDERS ARE

TRYING TO HELP, BUT THAT'S THE

FIRST PLACE TO START.

>> YOU MENTIONED KICKING OFF

YOUR INCIDENT RESPONSE PLAN.

I'VE SEEN A MA CHIEWRKS TESTED
INCIDENT RESPONSE PLAN IS
PIVOTAL TO DEALING WITH A
RANSOMWARE ATTACK.
I THINK WE'VE PICKED UP THREADS
THROUGHOUT DIFFERENT
CONVERSATIONS TODAY THERE ARE A
LOT OF VARIANCES AND NUANCES TO
THE TYPES OF ATTACKS OUT THERE
AFFECTING CLIENTS TODAY AND
OTHER VICTIMS.
SO UNDERSTANDING THE NUANCES OF
EACH OF THOSE AND WHICH ONE HAS
TARGETED YOUR ORGANIZATION CAN
BE LIKELY CRITICAL.
YOU MAY BE INFECTED WITH A
VARIANT THAT MAPS OUT AND
INFECTS -- IT NEVER SHARES.
YOU MAY BE INFECTED WITH THE
VARIANT THAT HAS A PUBLISHED
DESCRIPTION KEY FOR IT.
SO BUILDING THAT CAPABILITY INTO
YOUR INCIDENT RESPONSE PLAN SO

YOU CAN FOCUS IN ON THE VARIANT
YOU HAVE BEEN ATTACKED WITH CAN
BE CRITICAL TO YOUR SUCCESS.
>> SPEAKING OF THE VARIANTS,
PAAÄIVI, YOUR COMPANY F-SECURE
LOOKED AT A LOT OF DIFFERENT
VARIANTS AND THE COOP ASSUMER
EXPERIENCE WITH THE VARIANTS,
WHETHER IT BE WHAT KIND OF
LANGUAGE DO THEY COMMUNICATE IN,
WILL THEY NEGOTIATE ON THE PRICE
OF THE RANSOMWARE, GIVE YOU
EXTENSIONS OF TIME.
COULD YOU SHARE A LITTLE ABOUT
THAT REPORT AND WHAT YOU GUYS
FOUND?
>> YEAH, YOU ACTUALLY SET OUT
PRETTY MUCH EVERYTHING WE WERE
DISCUSSING IN THE REPORT, THAT
WAS QUITE A LOT.
SO I'LL PROBABLY START START
WITH THE LANGUAGE SUPPORT.
AS WE SAW IN THE PRESENTATION

EARLIER, THE LANGUAGE OF THE
RANSOMWARE NOTE CAN BE BASED ON
THE COMPUTER LOCAL LANGUAGE OR
WHAT IS THE HE BOARD SETTINGS.
BUT USUALLY WHAT THEY LOOK FOR
IS THE I.P. ADDRESS.
SO THEY CAN PRESENT THE
RANSOMWARE NOTE ON YOUR OWN
LANGUAGE.
FOR EXAMPLE IF YOUR I.P. ADDRESS
IS LOCATED IN GERMANY, THE NOTE
IS PRESENTED TO YOU IN GERMAN.
AND --
>> WHAT ABOUT A NEGOTIATING
PRICE?
WHAT KIND OF FINDINGS DID YOU
HAVE WITH RESPECT TO PEOPLE
HAVING SUCCESS GETTING THE LOWER
PRICE THAN THE PRICE THEY ASKED
FOR INITIALLY?
>> ACTUALLY, IN THE RESEARCH, WE
WERE STUDYING FIVE DIFFERENT
VARIANTS.

SOME WERE MORE PREVALENT THAN

THE OTHERS.

ALL OF THEM WHO RESPONDED TO OUR

QUERIES, THAT WAS FOUR OUT OF

THE FIVE VARIANTS, WERE

EXTENDING THE DEADLINE, AT

LEAST.

THREE OUT OF THE FIVE VARIANTS

LOWERED THE PRICE.

IT WAS ON AVERAGE 29%.

>> WILL, BEFORE WE HAD THIS

PANEL, YOU AND I WERE TALKING

BRIEFLY ABOUT THE ABILITY TO GO

ONLINE AND TRY TO FIND ONLINE-LINE AND TRY TO FIND ON-LINE

DESCRIPTION KEYS AND TRYING TO

AVOID HAVING TO INTERACT

DIRECTLY WITH THE RANSOMEWARE

AGENT BY GETTING THESE

ENCRYPTION KEYS AND YOU TOLD ME

ABOUT THE EXPERIENCES SOME

PEOPLE HAVE HAD WITH THOSE

ON-LINE ENCRYPTION KEYS.

COULD YOU SHARE THAT.

>> SURE.

WHILE I DO ENCOURAGE PEOPLE TO

DO A LOT OF OPEN SOURCE RESEARCH

IF THEY ARE VICTIMS OF

RANSOMWARE EVENTS, A LOT HAS

DONE AND SO PLEASE DO RESEARCH

ABOUT THE VARIANT YOU YOU MIGHT BE

ATTACKED WITH BUT BE EXTREMELY

SKEPTICAL WITH THINK

INTERACTIONS WITH ANY COMPANY

THAT SAYS THEY HAVE A DECRYPTER

AVAILABLE WHERE EVERYBODY ELSE

IS SAYING THEY DO NOT HAVE A

DESCRIPTION TOOL AVAILABLE.

YET THIS ONE OR TWO OR WHATEVER

COMPANY HAS THE TOOL AVAILABLE.

WHAT WE HAVE SEEN IS SAID

COMPANY OR COMPANIES ARE MORE

THAN LIKELY JUST INTERFACING

WITH THE SUBJECT.

AND PAYING THE RANSOM FOR THE

VICTIM, CHARGING THE VICTIM OF

COURSE AND JUST OBTAINING THE

DECRYPTION KEYS FROM THE
RANSOMWARE SUBJECT, HIM OR
HERSELF.
AND THEN CREATING THE
QUOTE/UNQUOTE DESCRIPTOR CODE
FOR THE DECRYPTION KEYS
PROVIDING TO THE VICTIM.
IT'S THEY THOUGHT THEY WERE UNITED
AGAINST THE CAUSE NOT PAYING THE
RANSOM, THEY'RE JUST CHARGED
THIS FEE FOR THIS DECRYPTION
TOOL HOWEVER THEY ULTIMATELY
WENT THROUGH THIS MIDDLEMAN
COMPANY THAT PAID THE RANSOM AND
WE HAVE SEEN THAT.
>> ACTUALLY I THINK IT WOULD BE
PRETTY SUSPICIOUS IF THE AMOUNT
YOU PAY FOR THIS COMPANY WHO IS
PROVIDING YOU THE DECRYPTION
TOOL IS PRETTY MUCH THE SAME OR
MORE THAN WHAT THE EXTORTIONISTS
WERE ORIGINALLY ASKING FOR.
>> RANSOMEWARE IS VERY MUCH A

BUSINESS MODEL.

SOME ARE BETTER AT IT THAN

OTHERS.

>> THERE'S CERTAIN ORGANIZATIONS

I GET THAT RELEASED ALL THE KEYS

ASSOCIATED WITH THAT SO THAT

BECAME PUBLIC.

>> AS LONG AS YOU'RE

RESEARCHING, FOR EXAMPLE THE FBI

RELEASED THE PANEL ON THAT

BECAUSE THE SUBJECT DID RELEASE

THE MASTER DECRYPT KEY FOR THAT

FOR VERSION THREE I THINK IT WAS

AND ON.

AS WELL AS IT IS WORTH NOTING

THAT SOME OF THESE OTHER

VARIANTS THAT ARE OUT THERE,

THERE'S QUOTE/UNQUOTE

PROFESSIONAL ONES THAT ARE KIND

OF THE HEAVY HITTERS AND THERE'S

OTHER ONES THAT ARE MORE AMATEUR

LEVEL THAT HAVE THE FLAWS THAT

DECRYPT ION TOOLS ARE MADE

BECAUSE OF THOSE FLAWS.

IF YOU ARE SUBJECT TO A

RANSOMWARE EVENT AND YOU'RE ABLE

TO RESTORE FROM BACK UP, YOU CAN

PUT YOUR FILES OFF TO THE SIDE

AND THERE MIGHT BE A DECRYPTION

TOOL AVAILABLE IN A FEW WEEKS,

MONTHS, MAYBE YEARS.

BUT IT'S WORTH NOTING.

>> I THINK AGAIN ONE OF THE KEYS

TO UNDERSTAND IS SOME THREAT

INTELLIGENCE, WHAT EXACTLY ARE

YOU DEALING WITH.

SO UNDERSTANDING YOUR RANSOMWARE

VARIANT AND THEN THROUGH THAT

THEN DETERMINING YOUR NEXT STEPS

ASSOCIATED AGAIN FROM A

CONTAINMENT ASPECT OF IT.

ONE THING THAT WE'VE BEEN SEEING

A LOT OF RECENTLY NOW, A LOT OF

PANELISTS WERE TALKING EARLIER

ABOUT HOW RANSOMWARE GETS

INITIATED, COMING THROUGH PHISH

AND WE'VE SEEN IT COME THROUGH

RDP.

AGAIN A NEW ATTACK FACTOR THAT'S

OUT THERE.

IT'S NOT USER INITIATED.

THE ATTACKER'S ACTUALLY GET ON

TO AN RDP, GETTING ON TO THE

SERVER AND THE ATTACKER'S

ACTUALLY INITIATING IT

THEMSELVES.

SO IT'S ALWAYS GOOD TO

UNDERSTAND EXACTLY HOW IT GOT

WITHIN THE ORGANIZATION.

>> THAT LEADS ME TO MY NEXT

QUESTION WHICH IS SO LET'S SAY

YOU'VE GOTTEN THE MESSAGE, YOU

GOT THE SKULL AND CROSS BONES,

YOU'VE DONE THE CPR,

DISCONNECTED THE MACHINE FROM

THE NETWORK IMPORTANT TO LAW

ENFORCEMENT.

CAN'T FIND A DECRYPTION KEY OR

RELIABLE DECRYPTION KEY AND NOW

YOU HAVE TO DECIDE WHETHER YOU
WILL PAY OR NOT.
SHOULD YOU PAY OR MAYBE YOU'RE
THE FIRST ONE TO RESPOND TO
THIS.
WHAT'S THE F.B.I. POSITION
WHETHER YOU SHOULD PAY.
>> THE F.B.I. POSITION IS WE DO
NOT CONDONE PAYMENT, WE DON'T
SUPPORT IT.
HOWEVER WE VERY SYMPATHETIC IN
UNDERSTANDING AND WE WANT TO BE
ABLE TO WORK WITH YOU, BUT LIKE
MR. WRIGHT SAID AT THE LAST
PANEL SUCCESS BREEDS SUCCESS.
SO IN PAYMENT OF THESE RANSOM,
IT'S ONLY ENCOURAGING THEM TO
CONTINUE THEIR BUSINESS MODEL
AND EXTORT THE NEXT PERSON.
>> SOMETHING ELSE TO CONSIDER IS
IF YOU DO MAKE THAT, AS YOU'RE
MAKING THAT DECISION WHETHER OR
NOT TO PAY REMEMBER YOU'RE

DEALING WITH UNETHICAL PEOPLE.

THEY'RE NOT NECESSARILY GOING TO

HAVE OPEN AND FAIR BUSINESS

PRACTICES.

I CAN IMAGINE A SCENARIO WHERE

SOMEONE HAS BEEN ABLE TO SPREAD

A VARIANT OF RANSOMWARE TO A LOT

OF VICTIMS AND COLLECTED

DECRYPTION KEYS AND LOST HIS

INFRASTRUCTURE THAT HOSTED THOSE

DECRYPTION KEYS DUE TO A HOSTING

COMPANY IDENTIFYING THIS IS

INVOLVED IN TRAFFICKING AND

TAKING IT DOWN.

HE'S NOT GOING TO ADVERTISE HE

NO LONGER HAS ACCESS TO AT THAT

TIME DECRYPTION KEY.

BUT HE VERY WELL WILL TAKE YOUR

PAYMENT, YOUR ANONYMOUS PAYMENT.

SO I THINK YOU HAVE TO HAVE NO

EXPECTATIONS WHEN YOU GO INTO

THAT TRANSACTION AND THAT'S GOT

TO BE A KEY CONSIDERATION.

>> THAT'S A REALLY IMPORTANT
POINT TO MAKE SURE YOU DON'T
HAVE EXPECTATIONS GOING TO.
I WOULD SAY IN OUR EXPERIENCE
OVER 50% BUT UNDER 80% OF THE
TIME THAT PAYMENT RESULTS IN A
SUCCESSFUL DECRYPTION KEY GOING
BACK AND CLAIMING THEY HAVE SOME
MORE DATA AND SOME STATS AROUND
THAT.
SOMETIMES WE FILED THAT IT'S
THROUGH NO FAULT OF THE
ATTACKER.
WE'VE HAD FILES THAT HAVE BEEN
ENCRYPTED MULTIPLE TIMES BECAUSE
THE PERSON THAT ORIGINALLY GOT
THE E-MAIL SENT IT TO SIX OF
THEIR FRIENDS SAID HEY I CAN'T
OPEN THIS CAN YOU TRY AND THE
FILES JUST KEPT ENCRYPTING
THEMSELVES.
WE'VE SEEN FILES GETTING
CORRUPTED DURING THE ENCRYPTION

PROCESS AND THERE'S NO WAY TO
DECRYPT IT EVEN WITH A VALID KEY
AND WE'VE SEEN ATTACKERS SENDING
IN A KEY THAT WASN'T NECESSARILY
THE KEY FOR THE FILES YOU GOT.
ONCE YOU PAY THAT MONEY, THE
WHOLE IDEA BEHIND BITCOIN AND
UNTRACEABLE CURRENCY IS THERE'S
NO WAY TO GET THAT BACK.
I DON'T KNOW IF YOU HAVE ANY
MORE DATA.
>> UNFORTUNATELY WE DON'T HAVE
DATA ON THE PAYMENTS, WHETHER
IT'S THE DECRYPTION HAS BEEN
SUCCESSFUL.
>> ALSO, JUST KIND OF MORE ON
THE KNOW WHAT YOU'RE DEALING
WITH THE VARIANT, SAM SAM FOR
EXAMPLE WILL GIVE YOU A PRICE AS
SOON AS YOU WAY THAT THEY WILL
ALMOST DOUBLE IT AGAIN BEFORE
THEY GIVE YOU ACTUALLY THE
DECRYPTION KEYS.

ONCE YOU'VE MADE THAT PAYMENT,

THAT IS BASICALLY A COMMITMENT

TO THE SUBJECT SAYING WE HAVE NO

BACK UPS.

YOU HAVE A HOOK, LINE AND

SINKER.

IF YOU PAY THE RANSOM PLEASE

REPORT IT TO US, THERE'S NO

HOSTILITIES OR ANYTHING LIKE

THAT TO THE LAW ENFORCEMENT.

WE WILL GLADLY STILL SUPPORT YOU

HOWEVER WE CAN WITH OUR

INVESTIGATION.

>> I THINK IT'S A BUSINESS

DECISION.

AGAIN YOU HAD SOME EARLIER

PANELISTS TODAY.

WE'VE TALKING $700.

HOW VALUABLE IS THE DATA THAT

WAS IMPACTED TO THE

ORGANIZATION.

THEN FROM THERE PACIFIC IT, DO

WE HAVE NECESSARY BACK UPS AGAIN

FROM THE MEDIATION ASPECTS OF

IT.

THEN YOU HAVE TO DECIDE FROM A

BUSINESS PAY OR NOT PAY.

THERE'S A LOT OF ETHICAL

CONSIDERATIONS CONSIDERING SOME

OF OUR CLIENTS WE DON'T PAY.

WE DON'T, WE'VE BEEN RANSOMED

WE'VE BEEN HOSTAGED, WE DON'T

DEAL WITH TERRORISTS.

THE OTHER SIDE OF THE COIN IS,

IT'S A DEMINIMIS AMOUNT WE

ACTUALLY NEED THE DATA, WE NEED

TO PAY.

WHEN YOU GO THROUGH THAT PAYMENT

PROCESS IT GETS SCARY AND I

THINK EARLIER, EXCUSE ME LATER,

ADAM TALKED ABOUT BITCOIN

WALLETS AND HOW TO SET THAT UP.

WE'VE HAD A LOT OF CLIENTS

UNFORTUNATELY HAD TO PAY, THEY

HAVEN'T HAD THE BACK UPS

ASSOCIATED WITNESS.

THEY'VE BEEN SUCCESSFUL IN
RECOVERING THE DATA.
>> I THINK ONE LESSON TOO THAT I
LEARNED THROUGH AN UNFORTUNATE
ENCOUNTER WAS THIS COMPANY HAD A
VERY ROBUST BACK UP PLAN IN
PLACE.
IT WAS VERY WELL EXECUTED, DE
WAS PRESERVED BUT THEY DIDN'T
NECESSARILY DO THE JOB WITH
UNDERSTANDING WHAT DATA WAS
IMPORTANT TO THEM.
SO REMEMBER, THESE RANSOMWARE
EXECUTEABLES ARE GOING TO SEARCH
YOUR SYSTEM FOR ALL TYPES OF
FILE, EXTENTIONS.
AND THEY DIDN'T HAVE A BACK UP
POLICY AND THAT DATA WAS
IMPORTANT TO THE BRAND AND THERE
WAS A LOT OF BRAND IDENTITY THAT
WAS LOST EVEN THOUGH THEY DIDN'T
HAVE DATA THAT WAS REPRODUCED.
EVEN THOUGH YOU HAVE THOSE

DISCUSSIONS INTERNALLY WITH YOUR
DATA HOLDERS, DON'T JUST THINK
ABOUT FINANCIAL IS, DON'T JUST
THINK ABOUT STANDARD OFFICE
DOCUMENTS, THINGS OF THAT
NATURE.
ALL OF THE OTHER PLACES YOU
MIGHT HAVE STORED CRITICAL DATA
MAKE SURE THEY ARE PART OF YOUR
BACK UP POLICIES.
>> YOU GUYS MENTIONED PAYMENT BY
BITCOIN.
Y GOT A QUESTION HERE FROM THE
AUDIENCE THAT IS ASKING DOES
PAYING BY BITCOIN EXPOSE YOUR
ACCOUNT INFORMATION AND COULD
YOU BE SUBJECTED TO FURTHER
FRAUD BY PAYING BY BITCOIN AND
IS THERE A WAY TO PAY BY
BITCOINS IF YOU'RE DOING THE
RANSOM TO DO SO SAFELY.
>> I THINK SOME OF THE PLACES
YOU CAN PAY WITH BITCOIN ARE A

LITTLE BIT SKETCHY FOR LACK OF A
BETTER TERM.
THERE ARE LEGITIMATE WAYS OF
PURCHASING BIT COINS AND THEY
CERTAINLY WORK.
ONE OF THE THING THAT WE HAVE
NOTICED IS THAT SOME OF THE
ATTACKERS ARE EMBEDDING LINKS
AND MEANS OF PAYMENT INTO THEIR
MESSAGES SAYING HEY CAN YOU
BITCOIN, CLICK ON THIS LINK AND
BUY YOUR BITCOIN FROM THIS
LOCATION.
YOU'VE SEEN INSTANCES WHERE THAT
LINK WHERE ATTACKERS ARE
PROVIDING IN ORDER TO BE HELPFUL
IS THEN GOING TO HARVEST
ADDITIONAL BANK ACCOUNT
INFORMATION CERTAINLY HAS YOU
WOULD SIGN UP FOR THOSE
SERVICES.
YOU NEED TO JUST REMEMBER FROM
AN ATTACKER'S STANDPOINT, IT'S

ALL ABOUT MONITORRIZATION OF
DATA.
SO THE MORE DATA THAT THEY CAN
GET ABOUT YOU IN THE COURSE OF
THIS ATTACK, THE BETTER.
SO IF THEY CAN GET THE $700 FROM
YOU AND THEN IF THEY CAN ALSO BE
HARVESTING SOME ADDITIONAL
INFORMATION LIKE YOUR BANK
ACCOUNT INFORMATION, THEN ONCE
YOU PAY THEM 700, THEY CAN GO
BACK INTO YOUR BANK ACCOUNT AND
SEE WHAT ELSE WAS THERE.
SO I WOULD SAY NOT DIRECTLY.
CAN IT BE FROM A BITCOIN
PROVIDER.
IN ATM'S YOU CAN PUT IN CASH AND
GET BACK ELECTRONIC CURRENCY.
THERE'S THE PROBABILITY THAT THE
ATTACKER IS PROVIDING A
PARTICULAR ADDRESS THAT'S
PROBABLY NOT THE ONE THAT YOU
WANTED TO USE.

>> THAT LEADS ME TO ANOTHER

QUESTION.

IT SEEMS LIKE IF YOU PAY, THEN

THERE IS A RISK TOO THAT YOU

MIGHT END UP BEING ESSENTIALLY A

LEAD FOR OTHER SCAMS DOWN THE

ROAD BECAUSE IF THEY'VE GOTTEN

INTO YOUR MACHINE AND THEY'VE

BEEN ABLE TO ENCRYPT YOUR FILES,

MAYBE THEY'VE INSTALLED A KEY

STROKE, MAYBE THEY INSTALLED A

LATE INSTANT LINK SOMEWHERE THEY

CAN EXECUTE LATER ON.

THE FACT YOU PAID HOWEVER MUCH

MONEY THIS IS, $500 MAYBE $1,000

THEY KNOW YOUR FILES ARE VERY

VALUABLE TO YOU.

THEY KNOW THEY HAVE SOME MONEY,

THAT SOME INSIGNIFY UNLTD AMOUNT

OF MONEY AVAILABLE TO YOU TO

PAY, IS THERE A RISK YOU MIGHT

BE LIKELY TO BE REVICTIMMIZED IF

YOU'VE BEEN INFECTED AND PAY.

>> WELL, THE INTERESTING THING,
WILL, ABOUT THIS IS EVERYONE HAS
A CUSTOMER ID.
JUST LIKE ANY BUSINESS IF YOU'RE
GOING TO PAY, THEY HAVE THE ID,
THEY KNOW WHERE YOU'RE AT.
WE HEARD EARLIER LOCATIONS AND
VARIOUS OTHER THINGS.
YES, YOU COULD BECOME AN
INCREASING TARGET FOR OTHER
DIFFERENT TYPES OF CAMPAIGNS
THAT THIS PARTICULAR
ORGANIZATION MIGHT LAUNCH THAT'S
OUT THERE.
THEY CAN ALSO SELL DATA THAT
THEY HAVE TO OTHER ORGANIZATIONS
AND SAY HEY WE'VE GOT THESE GUYS
TO PAY, YOU MIGHT WANT TO TARGET
THEM AS WELL.
>> WE HAVE SEEN A COUPLE THINGS
THERE THAT WERE INTERESTING.
ONE OF THEM WAS NEED TO BE A
LITTLE BIT CAREFUL SOMETIMES THE

RANSOMWARE SITES ALLOW YOU TO

UPLOAD A FILE.

AND THE ATTACKERS WILL DECRYPT

THAT FILE FOR YOU AS A SIGN OF

GOOD FAITH AND A SIGN TO

DEMONSTRATE THAT THEY HAVE THE

ABILITY TO DECRYPT.

YOU HAVE TO CHOOSE THAT FILE.

IF YOU'RE GOING TO PAY CHOOSE

THAT FILE CAREFULLY BECAUSE IF

IT'S A FILE THAT HAS SOME

SENSITIVE DATA INSIDE OF IT, YOU

HAVE NOW VOLUNTARILY SENT THIS

FILE TO THE AWE TAXES --

ATTACKERS, YOU'VE NOW UP LOADED

IT TO THEIR WEBSITE.

IF THAT FILE HAS DATA INSIDE OF

IT THAT'S JUICY THEN THE

ATTACKERS LOOK AT IT AND GO OH

WOW MAYBE WE SHOULD CHARGE THIS

PERSON MORE OR MAYBE WE SHOULD

ATTACK THEM AGAIN.

THE OTHER THING WE'VE SEEN IS

THAT THE ATTACKERS ARE STARTING
TO EXFILTRATE SOME DATA AS
THEY'RE DOING THIS ENCRYPTION.
AND IT GETS INTO THAT FOLLOW
ATTACK CONCEPT.
THE EXFILTRATING OF DATA SO FAR
HAS BEEN FTP CREDENTIALS SO
CREDENTIALS TO FTP SITES,
CREDENTIALS TO SITES THAT MIGHT
BE STORED IN CASH ON YOUR
BROWSER AND BITCOIN WALLET
CREDENTIALS.
SO WHILE YOU'RE MANAGING THIS
WHOLE RANSOMWARE PROBLEM AND
FIGURING OUT AND GOING THROUGH
YOUR CPR AND YOU MENTIONED SOME
OF THAT RESPONSE, INSTANT
RESPONSE PLAN SHOULD BE MAKING
SURE THAT PART OF YOUR
CONTAINMENT EFFORTS ARE
CONFIRMING THAT ANY OTHER
CREDENTIALS THAT MIGHT HAVE BEEN
ON THAT MACHINE ARE NOT BEING

MISUSED OR ATTACKED THROUGH
ANOTHER VECTOR WHILE YOU'RE
DEALING WITH THIS WHOLE
ENCRYPTION PROBLEM.
>> JUST ON THE CPR ASPECT OF IT,
PRESERVATION OF LOGS, FIREWALL
LOGS ARE VERY CRITICAL,
ESPECIALLY IN OUR INVESTIGATIONS
BECAUSE IF THE RANSOMWARE IS
INITIATED BY AN INDIVIDUAL, WE
WANT TO SEE THE CONNECTION TO
THE COMMAND CONTROL TO COME
BACK.
WE ARE GOING TO SEE TRAFFIC BUT
IF WE CAN'T SEE DE MINIMIS
AMOUNT OF TRAFFIC WE KNOW THAT'S
THE KEY COMING BACK IN AS
OPPOSED TO DATA EXFILTRATED AND
LEAVING THE ORGANIZATION.
>> SO WE HAVE OBSERVED THAT THE
RANSOMWARE IS ACTING AS A BACK
DOOR ALSO SO THE RANSOMWARE
INFECTION ISN'T THE ONLY THING

GOING ON AND THE RANSOMWARE

COULD BE DOWNLOADING ADDITIONAL

MAL WARE.

FOR EXAMPLE, ADDING YOUR

INFECTED COMPUTER TO A BOTNET OR

DOWNLOADING QUICK FRAUD MAL WEAR

AND -- MAL WARE AND THESE SORT

OF THINGS.

THERE COULD BE ALSO THESE

CREDENTIAL STEALERS AND MAL WARE.

>> THERE ARE PUTTING OTHER

THINGS INTO THE BACK DOOR AND

COULD BE LAUNCHING LATENT

ATTACKS.

IS THERE A BEST PRACTICES FOR IF

YOU GET THE FILES UNENCRYPTED,

WHAT DO YOU DO WITH THAT MACHINE

OR MACHINES THAT HAVE BEEN

INFECTED.

DO YOU REMOVE THOSE FILES OR

THROW THAT COMPUTER OUT.

HOW DO YOU ENSURE YOU WON'T BE

HITTING IN BY SOMETHING.

>> I WOULD SAY THE, ONE OF THE
FIRST THINGS IS TRYING TO FIGURE
OUT HOW YOU GOT HIT IN THE FIRST
PLACE.
BECAUSE ONE OF THE, AND I'M SURE
ADAM AND BILLY, YOU HAVE THE
SAME ISSUES, ONE OF THE WORST
THINGS IS WHEN YOU GO THROUGH
THIS PROCESS AND YOU GO THROUGH,
YOU PAY THE RANSOM AND THEN YOU
TELL THE F.B.I. THAT YOU DIDN'T
PAY THE RANSOM AND YOU GET YOUR
FILES BACK MAGICALLY AND THEN
THAT USER GETS BACK TO THEIR
E-MAIL AND OPENS UP THAT E-MAIL
AND GOES OH YEAH I WAS TRYING TO
OPEN THIS AND THEN THEY TRIED IT
AGAIN.
AND IT'S JUST RINSE AND REPEAT.
SO IT REALLY IS IMPORTANT TO
MAKE SURE THAT YOU SANITIZED NOT
JUST THAT MACHINE POTENTIALLY
BUT ALSO WHATEVER INFECTION

VECTOR THERE WAS ORIGINALLY.

>> IF THE PERSON THAT INITIATED IT, IF THEY CAN BE GIVEN A CLEAN DEVICE AND THEN HAVE THEIR ORIGINAL DEVICE PUT OFF TO THE SIDE SO WE CAN INVESTIGATE WHAT'S GOING ON.

IT'S PROBABLY THE BEST COURSE OF ACTION.

ALSO IF IT CAME IN THROUGH E-MAIL, HAVING THE E-MAIL ADMINISTRATOR PULLING THE PAYLOAD OUT OF THE E-MAIL THAT'S PRESERVING IT IS ALSO A GREAT IDEA IS SERGE'S POINT.

PEOPLE WILL DO THINGS THAT MAKE YOU SCRATCH YOUR HEAD LIKE THE EXAMPLE HE JUST GAVE AND YOU GO BACK INTO IT AND WHEN REINITIATE IT AGAIN.

DOING THOSE THINGS CAN KIND OF HELP PEOPLE OUT AND IT COMES DOWN TO BEHAVIORAL ASPECTS.

SOMETIMES WE FORGET AND WE DO
THINGS AND SOMETIMES WE DO
THINGS AND WE'RE LIKE OKAY
WHAT'S GOING ON.
>> PAIVI MENTIONED EARLIER THE S
SECURE HAD A 29% AVERAGE
REDUCTION WHEN THEY NEGOTIATED
ON THE PRICE OF THE RANSOM.
I WAS CURIOUS OF SERGE ADAM AND
BILL, YOU'RE DEALING WITH YOUR
CLIENTS.
HAVE YOU NEGOTIATED, AND IF SO,
WHAT KIND OF SUCCESS HAVE YOU
HAD GETTING YOUR REDUCTION
RANSOM.
>> I THINK NEGOTIATION IS A
DOUBLE-EDGED SWORD WHERE WE HAVE
SEEN SOME EVIDENCE OF
NEGOTIATING BEING SUCCESSFUL.
I THINK WE'VE ALREADY HAD
ADMISSION IT CAN GO THE OTHER
DIRECTION AS WELL.
THESE PEOPLE COMMIT EXTORTION

FOR A LIVING SO THEIR GOAL IS TO
GET AS MUCH MONEY AS THEY CAN.
I THINK IT'S A VERY IMMATURE
MARKET TO SOME DEGREE.
THEY DON'T QUITE KNOW WHEN
PRACTICES WORK BEST AND WHAT IS
MOST PROFITABLE BUT YOU CAN
IMAGINE THERE'S ALSO SCENARIOS
WHERE YOU UNDERSTAND THEY'RE
TALKING TO A DESPERATE
ORGANIZATION, HAS A LOT OF
CRITICAL DATA AT RISK AND MORE
APT TO PAY A HIGHER DEMAND OR
HIGHER RANSOM.
SO I THINK THAT'S YOU KNOW KIND
OF, THERE'S NOT REALLY GOOD
ADVICE, I DON'T THINK, CLEAR
ADVICE THAT CAN BE FOLLOWED IN
EVERY CASE WHERE YOU'RE GOING TO
ENGAGE AND POTENTIALLY PAY A
RANSOM, BUT THE PRAGMATIST IN ME
THINGS YOU'LL BE BETTER GOING
THAT ROUTE.

>> THE KEY POINT IS IF YOU DO
ENGAGE ANY SORT OF COMMUNICATION
IN GENERAL WITH THE ATTACKERS,
EITHER DO IT THROUGH AN
INTERMEDIARY OR DO IT THROUGH AN
ANONYMOUS ACCOUNT.
JUST LIKE THEY'RE NOT SENDING
YOU E-MAILS FROM THEIR BUSINESS
ACCOUNT.
THEY'RE CREATING ANOTHER ACCOUNT
WHETHER IT'S GMAIL OR HOTMAIL OR
SOMETHING LIKE THAT SO THEY STAY
RELATIVELY ANONYMOUS.
IF YOU SEND THEM AN E-MAIL FROM
YOUR BUSINESS ACCOUNT SAYING HEY
CAN WE NEGOTIATE THE RANSOM ON
THIS, THEY CAN USE GOOGLE TOO
AND THEY PLUG IN THE BUSINESS
NAME AND THEY GO WELL I DON'T
KNOW, IF YOU'RE A MULTIBILLION
DOLLAR COMPANY YOU CAN
NEGOTIATE.
IT JUST WENT UP.

SO IF YOU CAN APPROACH THEM FROM
AN INTERMEDIARY INSTEAD, THAT
CAN HELP WITH SOME OF THOSE
NEGOTIATIONS IF YOU'RE GOING TO
DO IT TO SEE IF FIRST OF ALL IF
THEY RECOGNIZE WHAT THEY HAVE
BECAUSE IT COULD JUST TOTALLY BE
A RANDOM DRIVE BY RANSOMWARE AND
THEY'RE LOOKING AT IT TO MAKE A
QUICK BUCK AND DON'T DO THEIR
RESEARCH.
AND AT THAT POINT, SURE, IT WILL
CUT YOUR RANSOM AND HEY IF YOU
CAN PAY A THOUSAND DOLLARS WE'LL
TAKE A THOUSAND DOLLARS.
>> I THINK IN SOME OF OUR
EXPERIENCE TODAY, THERE ARE A
LOT OF INSURANCE COMPANIES THAT
ARE IN THE BREACH RESPONSE
BUSINESS THESE DAYS AND MANY OF
THESE COMPANIES ARE STARTING TO
OFFER CYBER EXTORTION COVERAGE
UNDER THOSE POLICIES.

IF YOU HAVE BREACH INSURANCE YOU
MIGHT WANT TO ENGAGE YOUR
INSURANCE PROVIDER IF THAT'S
MADE BY YOUR ORGANIZATION TO SEE
IF THAT'S A SERVICE COVERED BY
THAT PROVIDER.
>> SPEAKING OF BREACH
INSURANCING SOMETHING THAT SMALL
BUSINESSES MIGHT DO IN RESPONSE
TO RANSOMWARE.
ARE THERE OTHER ISSUES RELATED
TO SMALL BUSINESS RELATED TO
RANSOMWARE LIKE REPORTING TAX
ISSUES.
>> NOT REALLY SURE HOW YOU BOOK
I PAID RANSOM FROM A FINANCIAL
STANDPOINT.
BUT WE'VE RUN INTO A COUPLE
INTERESTING QUESTIONS.
FOR BUSINESSES THAT MIGHT HAVE
REQUESTS FREEDOM OF INFORMATION
ACT, THE SUNSHINE LAW ACT
REQUESTS OR REQUESTS THAT MIGHT

BE HUGE TO HIPAA REQUIREMENTS,
THERE'S ALWAYS QUESTIONS AROUND
IF DATA'S ENCRYPTED, IF YOU
DON'T PAY THE RANSOM, YOU CAN'T
GET THESE FILES BACK AND YOU
THEN GET A LEGAL REQUEST AT SOME
LATER DATE AND SAY HEY DO YOU
HAVE INFORMATION ABOUT X.
ARE YOU OBLIGATED TO SAY WE
MIGHT HAVE, BUT NOW WE CAN'T
ACCESS IT ANYMORE SO WE CAN'T
PRODUCE IT.
SO IT DOES AS AN ADDITIONAL
LAYER OF COMPLEXITY INTO THINGS
FOR INTERESTS.
HIPAA CERTAINLY THE CMS GUIDANCE
IS THAT RANSOMWARE IS CONSIDERED
A BREACH UNLESS YOU MEET THESE
FOUR TIERS OF REQUIREMENT TO
UVMENTMALS IT WASN'T ACCESS.
THAT'S WHERE BILL, ADAM IF YOU
GET INTO RESPONSE OF THINGS
THAT'S REALLY WHAT WE'RE TRYING

TO LOOK AT AND HELP ASSESS
WHETHER OR NOT THE DATA'S BEEN
ACCESS.
OR LIKE PAIVI WAS SAYING IF THE
ATTACKERS PUT SOME ADDITIONAL
MAL WARE ON THE SYSTEM YOU HAVE
ACCESS AS WELL AS ENCRYPTION
PROBLEM.
>> FROM A BITCOIN PERSPECTIVE
HOW DO YOU PUT THAT ON THE
BOOKS.
IS IT A SHORT TERM CASH ACCOUNT,
BITCOIN FLUCTUATES JUST LIKE A
FOREIGN CURRENCY TRANSACTION,
HOW DO YOU DO THE ACCOUNTING
ASSOCIATED WITH THAT.
WHOSE NAME IS GOING TO BE IN THE
BITCOIN WALLET.
THOSE ARE THINGS YOU'RE GOING TO
THINK ABOUT IF YOU'RE GOING TO
GO DOWN THAT ROUTE.
>> I'VE GOT QUITE A FEW
QUESTIONS FROM THE AUDIENCE HERE

INGOES BACK TO THE QUESTION WE HAD

ABOUT WHETHER YOU SHOULD PAY.

IT SAYS IS RANSOMWARE SUCCESSFUL

BECAUSE THE PUBLIC BELIEVES

THEY'LL GET THE DECRYPTION KEY.

CAN RANSOMWARE BE DISRUPTED BY

TELLING PEOPLE THAT PAYING DOES

NOT WORK.

I GUESS THAT GETS BACK TO THE

F.B.I.'S POSITION ON PAYMENT

HERE AND SORT OF THE PUBLIC

POLICY IMPACT OF TELLING PEOPLE

EITHER TO PAY OR NOT PAY TO I

GUESS SERGE ADAM AND BILL YOU

DEAL WITH CLIENTS THAT FACE THIS

DECISION ABOUT WHETHER TO PAY.

HOW OFTEN DO THEY CONSIDER THE

QUESTION ABOUT WHETHER MAYBE

IT'S THE BEST THING IN MY

INDIVIDUAL CASE TO PAY BECAUSE I

WANT MY FILES BACK.

BUT IF IF I PAY, I'M FUNDING THIS

OPERATION AND PERPETUATING

RANSOM.

>> IN THE REMEDIATION SIDE OF THE HOUSE, HOW VALUABLE IS THE DATA AND DO WE HAVE THE PROPER MECHANISMS TO RESTORE THAT DATA.

SO, LET'S PRETEND WE CAN'T RESTORE THE DATA.

HOW VALUABLE IS IT TO YOUR ORGANIZATION AND I THINK YOU PUT IN A BUSINESS CONTEXT IF IT'S VALUABLE WE CANNOT CONTINUE THE OPERATION.

ADAM FOR EXAMPLE LIKE WITH THE VIDEO FILE, VERY VALUABLE TO THE ORGANIZATION, THEY DIDN'T HAVE ANY BACK UPS AND IN THAT CASE THE BUSINESS HAS TO DECIDE DO WE PAY 700, $800,000 TO GET OUR DATA BACK AND THE ANSWER WOULD BE YES, YOU NEED TO PAY.

BUT THEN AFTER WE PAY, WE NEED TO MAKE SURE WE GOT OUR HOUSE BACK IN ORDER IN THESE BUSINESS

CONTINUITY PLANS AND EVERYTHING
ELSE WITHIN THE ORGANIZATION TO
NOW ADDRESS THIS THREAT.
>> ARE YOU SUGGESTING THAT YOU
TRY TO SEE PEOPLE AND SAY IT
WON'T WORK.
THE ATTACKERS HAVE THE PERFECT
SOLUTION TO THAT IS THAT THEY'RE
HAPPY TO SHOW YOU IT WORKS.
YOU HAVE A WEBSITE, YOU CAN
UPLOAD A FILE TO IT AND YOU CAN
DECRYPT IT.
INSTEAD OF SAYING NO, NO IT
WON'T WORK.
THE ATTACKERS CAN DELETE AND GET
AROUND THAT AND MORE TO THE
POINT OF IF YOU GET STUCK ONCE,
MAKE SURE YOU DON'T CLICK ON THE
E-MAIL AGAIN.
>> SOME OF THESE GUYS ACTUALLY
HAVE CUSTOMER SERVICE
REPRESENTATIVES TO HELP YOU OUT.
AGAIN, IT'S A BUSINESS TO THEM

AND IT'S VERY SUCCESSFUL AND
MAKING A LOT OF MONEY DOING IT.
>> IT IS, IT'S SOMETHING ELSE,
ANOTHER REASON TO ENGAGE WITH
LAW ENFORCEMENT TOO.
WE DEALT WITH A FEW OF THESE
WHERE THE WEBSITE THE PERSON
WENT TO WAS THEN LED TO THE MAL
WARE WAS A PERFECTLY LEGITIMATE
BUSINESS SITE THEY HAD TO GO TO
AS PART OF THEIR NORMAL BUSINESS
OPERATION.
SO IT'S NOT LIKE YOU COULD TELL
THAT PERSON DON'T GO TO THIS
MEDICAL SITE ANYMORE.
BECAUSE IT WAS THEIR JOB TO GO
TO THE MEDICAL SITE AND PULL THE
DATA OFF THAT SITE AND GO
SOMEWHERE ELSE.
IT WAS IMPORTANT TO TURN THAT
INFECTION ABOUT THAT INFORMATION
VECTOR OVER TO THE FBI SO THEY
COULD CALL THAT HOSTING COMPANY

AT THE END OF THE DAY AND SAY

HEY YOU GUYS HAVE A PROBLEM WITH

YOUR WEBSITE, ADDRESS IT.

AND MAKE SURE THAT OTHER PEOPLE

DON'T GET VICTIMIZED BY IT.

IT'S JUST ONE MORE REASON.

>> THIS QUESTION WILL BE

DIRECTED TO THE F.B.I.

HOW FREQUENTLY -- IS THIS A GOOD

DEED FOR INDIVIDUALS -- WELL I

GUESS LET'S WALK IT BACK TO THE

FIRST QUESTION.

HOW FREQUENTLY DOES THE FBI

RESPOND IN INDIVIDUALS'

COMPLAINTS.

DOES THE FBI WORK ON THIS DAY TO

DAY, IS THIS JUST THEY'LL

CONTACT YOU, YOU'LL LOG IN THE

COMPLAINT AND THE FBI WILL USE

IT FOR ITS DATA GATHERING

PURPOSES IN ITS INVESTIGATION.

WHAT HAPPENS WHEN THE FBI

RESPONDS TO THESE INCIDENT

REPORTS.

>> I LIVE AND BREATHE RANSOMWARE

EVERY SINGLE DAY.

WE ARE FEELING SOME KIND OF

RANSOMWARE COMPLAINTS LITERALLY

EVERY SINGLE DAY THROUGH OUR 56

FIELD OFFICES.

AND THOSE ARE USUALLY EITHER

COLD CALLS OR BASED UPON

CONTACTS, RELATIONSHIPS THAT ARE

PREEXISTING WITH THE LOCAL FBI

AND ON TOP OF THAT WE HAVE OUR

IC3 PORTAL.

SO WHEN YOU MAKE THAT PHONE CALL

I CAN'T PROMISE YOU'RE GOING TO

HAVE AGENTS SHOW UP AT YOUR DOOR

OR ANYTHING LIKE THAT BUT

DEPENDING ON YOUR SITUATION IF

YOU'RE JUST DOING A PHONE CALL

TO RECALL I'M JUST A VICTIM OF

RANSOMWARE HERE'S MY INFORMATION

AND WE SAY THANK YOU VERY MUCH.

AND MAYBE PART OF THE SECOND

QUESTION IS, I HOPE THEY FEEL
GOOD, A GOOD DEED AT THE END OF
THE DAY BECAUSE YOU'RE
FURTHERING THE CAUSE IF IT'S AN
ONGOING INCIDENT AND THE
RESPONSE TEAM CAN QUITE POSSIBLY
PLUG INTO THE IR TEAM OR AT
LEAST GATHER INFORMATION IN THAT
ACTIVE SCENARIO.
SO EACH SCENARIO IS GOING TO BE
VERY DIFFERENT DEPENDING ON THE
RANSOMWARE INCIDENT AND
COMPLAINTS.
>> I CAN ADD SOMETHING TO THAT TOO.
IN MY PRIOR LIFE I WAS A
COLLEAGUE OF WILL'S AND THE
INFORMATION THAT VICTIM PROVIDE
IS CRITICAL TO BUILDING THAT
CASE IN PROSECUTORIAL PHASE OF
AN INVESTIGATION.
SO WITHOUT BEING ABLE TO FIND
THOSE PEOPLE AND GIVE THOSE
IMPACTFUL STORIES ABOUT WHAT

RANSOMWARE DID THEM, THAT'S THE
DIFFERENCE BETWEEN SOMEONE BEING
ARRESTED SERVING A YEAR IN JAIL
OR 20 YEARS IN JAIL SO THAT'S
ANOTHER WAY THOSE STORIES REALLY
COME IN AND DEFINE THE IMPACT TO
THE PUBLIC.
>> YOUR PREPAREDNESS CAN REALLY
CHANGE WHAT HAPPENS WHEN YOU
BECOME A VICTIM AND I THINK BILL
TOUCHED ON THE RIGHT AT THE
BEGINNING AND TO END IT TOO, THE
FIRST TIME YOU'RE TALKING TO THE
F.B.I. IS WHEN YOU FIRST GOT HIT
AND THE FIRST TIME YOU REACH OUT
TO YOUR COMPANY OR VENDOR IT'S
AFTER A RANSOMWARE EVENT, THEN
WHAT HAPPENS IS A LOT BIGGER
THAN IF THAT'S BEEN AN ONGOING
DIALOGUE IF YOU ENGAGE WITH THE
FBI OR LAW ENFORCEMENT
BEFOREHAND, YOU HAVE A GOOD
RELATIONSHIP WITH YOUR AV

VENDORS AND FORENSIC VENDORS AND
YOU'RE ABLE TO BUILD ON THOSE
RELATIONSHIPS AND IT'S A LOT
EASIER THAN WHAT HAPPENS IS MORE
OF A NON-EVENT IF IT'S THE FIRST
TIME YOU'RE TRYING TO GO THROUGH
THIS.
>> THANK YOU ALL VERY MUCH FOR
COMING, REALLY APPRECIATE ALL
YOUR TIME AND EFFORT AND ALL THE
INFORMATION YOU'VE BEEN ABLE TO
PASS ALONG.
I ALSO WANT TO KNOW TECHNOLOGY
SERIES THE NEXT WORK SHOP IS ON
OCTOBER 13 AT 1:00 ON DRONES AND
THE LAST ONE IS DECEMBER 7TH,
ALSO AT 1:00 AND THAT'S ON SMART
TV.
SO I HOPE EVERYONE CAN MAKE IT
TO THOSE AS WELL.
THANK YOU EVERYONE FOR COMING,
WE REALLY APPRECIATE IT AND HAVE
A SAFE TRIP HOME.