00:08

Thank you guys for joining us today this is the fourth or fifth time that

00:14

I've came out and worked with Sara and Jess and the crew here at Blackhawk

00:20

Bank to share some good stuff with you guys around what's going on in the world

00:24

of cybersecurity mr. Hale did a great job of setting everything up so I won't

00:30

double up on his stuff but that's what we're gonna talk about today what does

00:34

the world look like in 2019 from especially from a small business

00:41

perspective or just from a business perspective and I'm gonna try to bust

00:46

some myths for you guys in case you're holding out some old-school thoughts on

00:52

who you are and how you operate as an organization but then we're gonna get

00:57

into some of the big takeaways the the major things that you guys need to keep

01:02

in mind and work towards doing at your organizations or even if you're just

01:08

here you know to learn from a personal perspective some of the things that you

01:12

guys need to be aware of and do so my contact information is listed out up on

01:17

here phone number email address our company were based out of Madison South

01:22

Dakota not the cool fun large Madison over here are our sleepy little now

01:28

flooded seventy five hundred person town in South Dakota so that's kind of a some

01:36

background there there's a little background information on who we are and

01:39

what we do and if I was teaching the bank about information security stuff we

01:47

would talk a lot about people process and technology and these are the ways

01:50

that we protect information we protect them through processes that's your

01:56

governance that's your policy and your procedure and your plans right we

02:02

protect our information through technology those are the things that you

02:06

guys are going to probably think of when we talk about cybersecurity or

02:10

protection your firewalls your passwords your antivirus your intrusion detection

02:15

prevention stuff right the logical technology

02:19

controls that keep bad guys out but also through people and the big secret to

02:28

cybersecurity stuff is it's inherently fundamentally human based so when I

02:35

asked you guys about people processing technology and I say what do you think

02:40

is the weakest link here what do you guys gonna say always because you can

02:45

you know you can't really convince a firewall for example to break the rules

02:52

that it's been programmed to follow firewall doesn't know how to do that

02:56

but you can train a person or ask a person or build a procedure around how

03:03

to do a process like like Hale was talking about up here with business

03:08

email compromised or Dave was talking about earlier you know sending out email

03:13

saying hey I need you to do this wire transfer or I need you to do this thing

03:17

for me and you can train people to say don't do that don't click links don't

03:25

blindly follow words on a screen ask questions but what's more likely to

03:32

happen a person breaking the rules that they've been asked to follow or a

03:37

firewall breaking the rules that it's only been programmed to follow right so

03:43

that's what we talk about when we talk about people process and technology but

03:47

people are oftentimes our biggest weakness or our biggest risk but with

03:53

good training with good education with the addition of some technology controls

03:58

we can mitigate that risk a bit you're never gonna be able to fully mitigate

04:02

any risk with information security right especially if bad guys decide that they

04:08

want to target somebody then they have nothing but time and a million different

04:14

avenues to try to get your information or get access to your stuff you know

04:20

that's that's kind of the scary part you know when it comes to the defense of the

04:27

defensive part of information security you know we have to keep

04:30

everything out including people from clicking on emails and letting folks in

04:36

the back door and and we have to be aware of all of this stuff bad guys only

04:40

need one opportunity right so just as a quick question in case you're you're not

04:47

quite sure that the impact of what we're talking about here if I sent every

04:52

person at your organization one phishing email every day how long would it before

05:00

I got one person to click on a link half an hour day one and and that's that's

05:10
the point right so we have to talk to our people we have to train them we have
05:15
to help them understand what's going on because if they don't even understand
05:20
what the world of phishing emails looks like and the impact that can have on a
05:25
business or an organization then then how are we expecting them to really be
05:30
our first line of defense so if if people are our biggest weakness when it
05:36
comes to security how do we turn that into good defense as opposed to just a
05:42
big weakness right sort of like in sports right you know everybody talks
05:50
about shoring up your weaknesses in sports well you got to practice you have
05:54
to put in the work you have to put in the time they have to be aware that
05:56
that's a weakness in the first place so so this is again just some about what we
06:01
do and where we work in the information security lifecycle what we don't do just
06:06
for you guys out there is we don't do any technical implementation stuff so we
06:12
help businesses understand risk and do a lot of training and education and build
06:17

governance build business continuity incident response plans stuff like that

06:22

and then we make decisions on how to protect but we don't manage firewalls we

06:27

don't host the data center we don't build servers and and patch networks or

06:33

any of those things but then on the backend we also do testing as the kind

06:39

folks here at Blackhawk Bank said you know we're we're a risk management and

06:43

audit firm really so we don't do any of that

06:46

technical implementation stuff but what we're gonna talk about here is some of

06:51

the top cybersecurity threats of today commercial account takeover much like

06:56

hail and David talked to you guys about a little bit already and then we're

07:03

going to talk about those 10 critical security controls for small business at

07:06

the end so there's a couple things and a couple big themes that I like to talk

07:11

about and a lot of this stuff gets really scary real fast and everybody

07:17

starts getting real nervous and talking about just unplugging the internet from

07:23

businesses or your home or whatever the case is but why do we have this stuff in

07:29

the first place does it makes things a lot more convenient and efficient for us

07:35

to do business right keep in mind that there's always risk in everything I'm

07:42

gonna jump in 1.5 tons of metal and rubber and hurdle myself down you know

07:49

some concrete and blacktop on the tollway back to o'hare and then I'm

07:55

gonna jump on a plane filled with you you know jet fuel and fly back to South

08:00

Dakota there any risk in that why do we do it

08:04

especially when you drive this toll away but why do we do that stuff sure beats

08:12

walking that's exactly right so keep in mind there's always risk and

08:17

we've we've got to apply the same risk management processes that we use for

08:23

every other area of our world you guys all do risk management on a day to day

08:28

basis you might just not really know it right with a car what are the ways that

08:33

we mitigate risk in a vehicle because there's the ultimate risk right I heard

08:39

seatbelts what else airbags what else maintenance what else what was that

08:48

yeah traffic signs roads right exactly what was the other thing right exactly

08:56

awareness about some of that stuff too don't text and drive

09:00

to the auto manufacturers do you crash testing to help ensure the security of

09:05

that car you know who's got a car that was built within the last two to three

09:10

years quit show hands how many computer sensors do you think are on those cars

09:15

these days a brand new Tesla for example has over 230 sensors on it you know one

09:23

of those automatic you know getting ready to be Auto driving cars crossing

09:29

my fingers for those days but so there's a ton of ways that we mitigate risk just

09:37

in our cars and it's the same thing in the technology products and web

09:43

applications and network devices and all of the things that we do at our

09:48

businesses today there's always a way to mitigate the risk right because the

09:53

alternative is we don't mitigate risk and bad stuff happens or we unplug the

09:59

internet and we go back to doing everything on pencil and paper so the

10:04

other thing to keep in mind when we talk about the world of cyber security today

10:10

is that this stuff is all automated right the the big myth that I hear a lot

10:19

or the lie that we like to tell ourselves is our a small organization in

10:27

the middle of nowhere we don't have anything that a bad guy wants right

10:33

nobody knows who we are nobody's gonna target us we don't have

10:37

enough value our business isn't big enough for bad guys to go after and it's

10:42

all a lie because bad guys don't know or they usually don't care until after

10:51

you've been compromised you know dave was talking earlier this

10:55

morning about an organization that got hit with an email compromise and he

11:00

didn't say that bad guys got in stole some money and got out it

11:05

wasn't a quick smash and grab right but they probably weren't targeted as an

11:11

organization and if they were you know they were just they got simply blasted

11:14

with some phishing emails but the big secret to all cyber security stuff these

11:21

days is bad guys don't typically know until after they get in so the question

11:28

I want to you guys didn't understand is what do you look like to a bad guy on

11:33

the internet my mascot if you heard me talk before is Boris the Ukrainian

11:38

hacker dude right so that's kind of the guy that we think of you know over in

11:43

the Ukraine just sitting in his in his hole you know working on his hacker

11:48

keyboard or a hacker laptop which is you know probably not really what is more

11:53

like an office building more like this probably but he's not over there just

11:58

simply typing in IP addresses into a command prompt and seeing what's alive

12:04

on the internet manually all the time right but how do you guys connect to the

12:12

internet like what's what's your identifier what's your business's

12:15

identifier on the Internet or any other device that you have that's

12:20

connected to the Internet it's simply an IP address right this is

12:24

an internal IP address but you get the picture right it's just a set of numbers

12:28

that's what you are on the Internet who's got a phone smartphone I'm

12:33

probably everybody here right IP address whose car who can start their

12:39

car from their phone IP addresses right you guys got IOT devices at home things

12:45

that connect to the internet cameras Google homes or Amazon alexa's

12:51

or echos I guess smart toasters smart refrigerators anybody have one of those

12:58

refrigerators that has a camera in it so you can look at see what's in your

13:02

refrigerator when you go to the grocery store and figure out what you forgot

13:04

like it's a beautiful time to be alive guys

13:11

they all have IP addresses right everything that's connected to the

13:16

Internet has an IP address and this is how bad guys identify things so remember

13:24

bad guys are scanning constantly do I have this attacks today are automated

13:29

these are just some examples of some free software programs that you can use

13:34

to just scan the internet for stuff most of this stuff is free if you really want

13:41

to get into exploiting things you know then there's a little bit of a different

13:45

story but there's you know you can see just all of these different things that

13:50

the screenshots aren't gonna mean anything to you guys but bad guys

13:54

they're not just sitting around plugging away looking for IP addresses seeing if

13:58

it's you know something that's going to talk back to them on the internet and

14:01

then manually digging in the whole process is automated I talked about this

14:06

example a little bit last year but we recreated the experiment probably six

14:12

months ago so we built what looked like a Windows XP computer and connected it

14:21

directly to the Internet right what's significant about Windows XP that is

14:25

we're gonna be talking about here in four months with Windows 7 as well

14:31

they're going away right it's not gonna be supported by Microsoft any longer

14:35

Windows XP lost support from Microsoft back in 2014 they've patched they've

14:42

released some some major patches a couple different times but for the most

14:46

part not supported right what does it mean to not be supported and to not get

14:51

updates no more security patches why are security patches important because that

14:58

plug they plug the holes that bad guys use to get in right so we built what's

15:07

called a honeypot so it's a box that looks like Windows XP that says hey I'm

15:12

Windows XP on the Internet right and a bad guy when they see something on the

15:17

internet that says hey I'm Windows XP how big do you think their eyes get my

15:21

Ohh yeah getting into this thing so but we put

15:24

some monitoring software on it so we built a box that look like Windows XP

15:29

that had some monitoring software on it so we could see what happens and we

15:33

connected it directly to the Internet how long do you think before a Russian

15:37

IP address got root access to that device from the time that we plugged it

15:43

into the Internet 48 seconds I think was the number right Russian IP address

15:50

identified it so what does that tell you about how automated this stuff is bad

15:57

guys are constantly monitoring the internet like this is their job right

16:02

like that and they're really good at it so anytime a new IP goes active on the

16:07

Internet they get alerted now there's billions of IPs you know that are

16:14

connected to the Internet so they're not digging into every one of them but this

16:19

is you know but they've automated the process there too of not just this but

16:23

exploitation and I don't have this up there we use a program called Metasploit

16:27

right and if there's not a security patch and a known hole it's called a

16:33

vulnerability so there's a program called Metasploit that you can download

16:39

for free there's a paid version too but that's the job of Metasploit is to

16:44

exploit known vulnerabilities to get in and they've got just automatic ways to

16:49

do that so not only does their software just

16:53

scan the internet for IP addresses and then alert them when there are major

16:58

vulnerabilities that they can access you know you know then they get the red flag

17:04

to say hey we got a live one over here you know Windows XP you know we ran some

17:09

scripts we're in what do you want to do so that process is all automated and as

17:16

has been mentioned before a lot of what we're seeing today involves ransomware

17:21

and this is particularly significant to you guys that own operate managed work

17:28

at small businesses right small business folks quick raise hands in here Yeah

17:34

right good that's most of you so have you heard about the city things

17:38

that are going on the municipality the government attacks that are occurring

17:45

three cities in Florida paid about 1.3 million dollars in ransom within the

17:51

last six months Baltimore Maryland Atlanta Georgia major major cities in

18:00

the US that have had their city government shut down and we're talking

18:04

about you know like the ability to generate revenue through tickets you

18:12

know parking tickets you know in city tickets those types of things

18:17

transportation systems buses railways all kinds of different things you know

18:24

email all of that stuff Cleveland Hopkins International Airport was

18:28

affected 22 county governments in Texas there were just recently dozens of

18:33

clinics in Oregon dental clinics in Oregon and Washington I mean the list

18:39

goes on and on and on you know like I didn't know about the the ransom we're

18:43

at the school thing but there was another school in Arizona that that

18:47

happened to there was a university I think in New York but bad guys are

18:53

really starting to catch on over the last 12 months that they can get a lot

18:58

more money or at least ask for a lot more money from city governments and

19:04

businesses and things like that then they can just asking for 300 bucks from

19:09

in Bitcoin from a consumer right and that month that data is a lot more

19:16

valuable to businesses in a lot of cases there was I've heard of two very recent

19:24

attacks one was a transportation company in Arkansas and the other was the city

19:29

of New Bedford not Illinois but Massachusetts and both of the ransoms

19:36

were north of 5 million dollars the transportation company in Arkansas was

19:43

over six hundred Bitcoin that they asked for bitcoins at least has a couple days

19:50

go a little over $10,000 a Bitcoin so but in addition to this insurance

19:56

companies are paying the ransom and bad guys are catching on to this too what

20:01

happens when insurance companies start paying the ransom the rates go up

20:08

communism or not communism Jesus I'm commerce at its finest sir maybe but you

20:18

know like capitalism at its finest right there right

20:21

supply and demand now we got insurance companies paying ransoms I bet we could

20:27

double triple that so that's a problem but health care government

20:31

transportation managed service providers who here works with a managed service

20:35

provider to help manage your network right their managed service providers

20:41

are starting to be targeted - why would a bad guy target a managed service

20:44

provider more people to help pressure that managed service provider - to

20:53

either pay the ransom or whatever the case is that's what happened to these

20:57

clinics in Oregon there was a managed service provider in Washington State I

21:03

believe that was servicing 12 to 13 dental clinics and they got ransomware

21:10

these dental clinics couldn't do much of anything and they didn't even hear they

21:14

called the emailed they didn't hear from their managed service provider for seven

21:19

days and you look up the story it's I think this happened last week I read it

21:24

and the managed service provider then sent a letter out to all these companies

21:28

and said sorry we're closed we are not in business any longer we apologize but

21:36

that manager you know so there's some scary stories out here managed service

21:40

providers are fantastic they'll get me wrong I mean that's just an example of

21:46

the risk that we're seeing also attackers are getting in a lot of times

21:53

through vulnerable Remote Desktop protocols right I don't know if any we

21:57

got any tech folks here and really know what Remote Desktop Protocol is but it's

22:02

the ability for you're different computers - what was

22:05

that yes yes sir to be able to communicate with one

22:10

another you know when you're not on the same network and you know having that

22:14

port open having some right now it's very vulnerable there's a big

22:19

vulnerability going around called blue keep that is exploiting RDP but it's

22:24

also an internet facing protocol right so there's typically login and using

22:31

default credentials bad guys are getting in that way too as well so lots of

22:37

different things so that's just kind of the world of ransomware right now when

22:41

we talk about DDoS attacks who here has heard of a DDoS attack before so a DDoS

22:47

attack is just simply flooding a network or a device with so much traffic that it

22:53

can't handle it and shut in it shuts down so bad guys have been targeting

22:58

like global DNS servers over the last couple years and I don't know if this is

23:03

gonna really mean anything for you but you know you can see here tax really

23:09

started increasing in size if you guys heard of the term botnet before right so

23:15

a botnet is a network of computers that an attacker can remotely control and

23:21

over the last three or four years they've really been targeting IOT

23:25

devices because IOT devices whether it's smart refrigerators or cameras or Google

23:32

homes in Google X's or whatever the case is they don't come with inherent

23:37

security built in so they're typically pretty vulnerable so bad guys have said

23:41

holy cow the number of devices on the Internet has quadrupled in the last

23:46

couple years mostly due to these IOT devices and we're going to use those as

23:51

relays and we're gonna compromise them because most of those things have

23:56

default usernames and passwords right and a lot of times we don't change them

24:00

so then bad guys take those over and they can just send traffic doesn't

24:04

really even really matter what type of traffic it is they just send traffic so

24:09

you've seen a real big spike here and especially in the last three years 16 17

24:14

18 in terms of the size of these attacks so just as an example you know most

24:21

businesses have between you know depending on the size of your business a

24:26

10 megabit connection to the internet or or excuse me a gigabit connection right

24:34

10 gigs right up or down or whatever it is up to 25 maybe 50 you know if you're

24:39

on fiber it's maybe a hundred you know but that's one connection and you're

24:46

seeing these attacks just spike up over you know 160 you know into the terabit

24:53

range right so a thousand gigabits ish is a terrible terrible right so the

25:00

attacks are so massive that even global things are having trouble keeping up

25:06

with a lot of these different attacks so also password reuse is a big issue top

25:16

25 worst passwords of 2018 this is a real list it might not seem real but it

25:22

is absolutely real the other thing to keep in mind is a lot of times bad guys

25:29

will publish usernames and passwords in on servers for other people to go

25:37

download so anybody here ever got an email or a notice that one of your

25:43

accounts been compromised Equifax you know wherever else so those

25:50

things are your username and password is probably online for bad guys to or

25:56

anybody to go download and use and again just like we talked about earlier it's

26:02

not Boris sitting there using you know these ten different username and

26:08

passwords and trying to go manually login to wellsfargo.com

26:12

or facebook.com guess what they've built to do it for them applications right so

26:20

they just take a user list and they say here's a thousand websites go see if any

26:24

of these usernames and passwords can log in to any of these websites and they get

26:29

a couple hits boom that's how you get a count takeover

26:32

today right that's especially how we're seeing a lot

26:36

of email compromise happen so long passwords and don't be afraid to change

26:43

them every now and again anybody here use a password manager online what do

26:48

you guys use LastPass LastPass RoboForm dashlane awesome highly highly highly

26:56

highly highly recommend password managers now again we're gonna go back

27:03

to that there's always risk conversation right but you can control the risk

27:07

number one most of these password managers are extremely secure and they

27:12

know they have to be because it's a treasure trove for bad guys so there is

27:17

risk especially if you use an online password manager we use as an enterprise

27:21

at SBS LastPass as well love it but you can set standards right you can say hey

27:28

all of my employees will have 20 character passwords and you guys are

27:32

thinking holy cow you're a crazy person 20 characters here's the best part you

27:37

don't have to remember them you can just be characters right because in the

27:41

browser on your phone on the desktop you can have that stuff autofill you have to

27:47

enter a long a nice long secure master password to get into LastPass you know

27:53

and you can set it up so that it you know your users have to re-authenticate

27:57

every time their computer locks or whatever it is so that you know you have

28:01

more security there but it's a great way to help mitigate the risk and kind of

28:07

take the password out of the equation because you don't have to remember them

28:10

and they can be long and secure if you guys don't want to go that route well

28:14

I've got a thing on passwords later on so I'll save that a little bit if you

28:19

guys has anybody here ever heard of showed an Brian I like it can I use this

28:27

laptop too is it connected to the Internet can I just use a browser it's

28:33

that cool

28:36

Chrome all right can I just run in here and throw it up on the screen so show

28:45

Dan is billed as the search engine for the Internet of Things by the Internet

28:52

of Things we just mean stuff connected to the Internet right and so I'm gonna

28:56

show you a couple different things but this is just an example if we don't get

29:01

this working of remote desktop the desktop protocol perfect so this takes

29:07

just a minute get up here

29:12

nope my fingers are in the wrong keys

29:18

see if I tape this right no I didn't but okay so again the search

29:27

engine for the Internet of Things right well make this a little bit bigger so

29:30

you can guys can see what I'm doing up here

29:32

but I'll tape in just gonna type in a remote desktop right again remote

29:42

desktop protocol it'll help you you know and there's some different things you

29:45

can do currently there are 3.3 almost 3.4 million devices connected to the

29:51

internet that are running RDP on Windows right okay here's the other fun part

29:59

let's see can you guys see what I'm typing there admin - slash admin what do

30:10

you think I'm gonna search for here is a live screenshot of a server looks like

30:25

it's in China that we could log into right now how long did that take 15

30:33

seconds and now I've got a live server here in China that I could use to log

30:38

into through their RDP protocol using admin admin

30:46

that that law enforcement guys still here this this part here not illegal

30:55

right but going into it a little bit more so but this is the you remember how

31:03

I told you guys you know and bad guys automate this stuff Thank You mr. Brian

31:06

that's a really good example so it's not just me making stuff up there's a number

31:12

of other things that you can do you want a list of all default passwords for

31:15

every device ever created every network device

31:19

there's a list for you right they're also free now most of this stuff was

31:26

created with good intentions right what anybody here an IT guy yeah a couple

31:33

right so why would you be interested if you work in managed services or you work

31:39

in IT why would you be interested in default usernames and passwords because

31:44

if you got stuff that you need to try to get into if you're helping out a client

31:47

be pretty helpful right also pretty helpful to the bad guys so if you want a

31:53

list of hacking tools SEC tools got org top-25 hacking tools for use right now

32:00

so most of them for free there's a hacking tool kits there's a whole

32:04

operating system for doing hacking stuff which we use at SBS from a defensive and

32:12

you know helping out our clients perspective so it's kind of that give

32:17

and take lots of other stuff if you guys want to do some cool information

32:22

gathering like I did I'll show you here there's a website called the Oh cent

32:27

framework right and we talked about this a lot too big big picture there's no

32:35

such thing as privacy today there's not if you are online there there's no

32:41

privacy unless you have done you know absolutely everything that you could and

32:47

you're a fanatic about privacy stuff but who here uses Facebook who here uses

32:54

Amazon who here uses Google Maps right or whatever else the case is

33:00

all of the things that you don't pay for with money you pay for with data it's

33:09

that simple today and for the most part it's cool right I mean you know and

33:17

we're using stuff Google Maps knows more about me than

33:21

anybody else you know in my life including my wife right

33:25

Google Maps knows where I go where I like to go where I've been hit anybody

33:30

ever checked out you like your Google Maps Timeline you know those types of

33:34

things you know you can go back and look at the history Google Maps will tell you

33:37

what your favorite type of food is I mean you probably Google knows this and

33:42

probably won't tell you but you know all of those things you know which

33:46

restaurant have I eaten at the most in the last 10 years probably that we've

33:50

been using Google Maps I mean there's a lot of data out there about us and so a

33:56

lot of this data you know you can find through the OSINT framework for example

34:01

right you used to have to go to your local county courthouse to find a lot of

34:08

different information about the stuff that you pay in terms of taxes and and

34:12

all of that information right all the information that that the county has

34:18

about you you don't have to do that anymore because it's all online and you

34:22

can search for it and find most of this stuff some of it you got to pay for but

34:25

you know some of these other things so the Oh cent framework stands the OSINT

34:30

stands for open source intelligence right so just gathering information but

34:34

if you want to find user names or email addresses or domain names for businesses

34:38

or IP addresses social networks instant messaging they're people search engines

34:43

I'll show you an example of that public records business records all

34:47

types of things there's a website out there called buzz file and so I said hey

34:51

what's what can I search in Rockford you know that might be kind of cool the

34:56

Discovery Center Museum right in Rockford I thought that most of you guys

35:01

would probably have an idea of what that is so here's all the information you

35:05

want to know how much revenue the Discovery Center Museum of Rockford does

35:09

they do about two million dollars a year anybody here from the Discovery Center

35:11

of Rockford sorry if I told you you know they have about 78

35:16

employees now the other thing so if you're going to do some business

35:20

intelligence right this is a pretty good place to start

35:26

keep in mind that not all of this stuff is 100% accurate or always the most

35:34

up-to-date but that's kind of it's it's a really good starting place you want to

35:39

look up email addresses which may be handy you found a target that might be

35:43

interesting got you got a two million dollar organization got 78 employees you

35:47

got contact information over here we got an address we got a map that's a pretty

35:51

good start so how do I get a hold of these folks well I've got an email you

35:55

got a URL up over there so let's start looking up some email addresses so you

36:00

go to a website hunter dot IO and we start looking up well mo just put in

36:06

this domain and we find all of these different emails right so job job titles

36:13

names of employees if they can find it pretty good place how would this be

36:17

useful to a bad guy phishing emails you got it you guys are thinking like

36:23

hackers you know now we want to get a little bit specific and this is a good

36:29

example of how this stuff is not always 100% accurate because I am NOT Jo HN I

36:38

am jo n but my dad is Jo HN so pit bull and Spokeo and some of these other

36:47

people search things actually confuse my dad and I

36:51

he's jo hn l Waldman and I'm Jo n C Waldman so my phone number you guys saw

37:00

the phone number here on my powerpoint slide up front that's that guy this is

37:07

my parents old phone number from before they moved this was my old phone number

37:10

when I had a landline in Madison I don't know what that one is there's some email

37:15

addresses over here but my dad lives in Hartford and last I checked I was not 64

37:21

years old this is maybe a year ago so he's 65 but you know I was 1981 he's

37:27

nine 8450 for so just know that this

37:31

information is not a hundred percent accurate but it gets you pretty close so

37:37

anybody heard of the website have I been poned calm I highly recommend that you

37:42

guys go check this guy out it is an extremely legitimate website

37:47

developed by a very well known and respected security researcher in the

37:52

community by the name of Troy hunt so he put this website together and I don't

37:57

know how old the screenshot is but he this lists out about I mean the number

38:03

is probably much higher than that today you know billions of compromised email

38:10

addresses and passwords so but what you can do is and it sounds kind of fishy

38:15

right away so this is why I'm telling you it's ok you put your email address

38:19

in there and look up and see what email addresses or what accounts using that

38:26

email address have been compromised and I'll tell you the password that was used

38:30

you can also sign up to get alerts if these guys discover new what we would

38:37

call you know credential dumps right there are new credential dumps that

38:42

include your email address they'll alert you if anybody here through the Equifax

38:49

breach sign up because it's kind of weird but Equifax like farmed out all of

38:54

their information you know personal identity theft monitoring stuff to

38:59

Experian you know like their direct competitor so but Experian has I think

39:04

that's called Real ID or whatever ID notify excuse me and they do some dark

39:10

web monitoring or data breach monitoring there too so a couple different options

39:14

if you don't trust the have I been poned site you can check out that stuff as

39:19

well so that's kind of you know the landscape of what's going on today we've

39:25

talked about a little bit about commercial account takeover I'm not I

39:28

think you guys all have a pretty good idea of what commercial account takeover

39:31

looks like today a couple of quick statistics 40% 43% of all reported

39:38

breaches involve small businesses which is more than double any other

39:43

sector that has experienced breaches including healthcare and financial

39:47

institutions right small businesses are being targeted because they are not big

39:53

and large and regulated but they still have a lot of dollars and a lot of

39:59

employees and there's a lot of small businesses and they typically don't have

40:03

security or at least the security that some of the more regulated industries

40:07

have and you know the FDIC we talk about this because we work with a lot of

40:13

financial institutions lists out commercial account takeover is the

40:16

number one threat to both banks and businesses right because we talked about

40:20

earlier $600,000 lost due to email invoicing compromised stuff you know

40:26

that's a very typical business email compromise or commercial account

40:35

takeover tactic we see that one a lot that's a story that I tell a lot so

40:40

thanks for stealing my thunder Dave I'm just kidding it was a really good

40:44

example but how does commercial account takeover work so you know bad guys

40:49

target folks or in some cases they just send out emails and get access or

40:53

compromise folks then they install malware they try to in terms of

40:57

commercial account takeover get a hold of your online banking or email

41:02

credentials so then that way they can do stuff themselves in a lot of cases you

41:08

know they get in they get access to the email as Dave talked about you know what

41:12

the details that he didn't mention were a lot of times they'll sit and wait and

41:16

monitor email as he mentioned and then they'll see who their the the

41:22

organization your small business is getting invoices from and then not only

41:26

will they send fake invoices but then they'll block the actual contractor or

41:32

company that's sending the invoices so you stop seeing the actual stuff and

41:36

you're seeing the other stuff and much like when mr. Hale was talking about the

41:43

email addresses and the domain names you know maybe they'll switch around domain

41:48

names so on and so forth so it makes it look like it's coming from a similar

41:51

thing but if you're not paying attention and it's coming from you know

41:54

and not Blackhawk Bank dot com but Blackhawk Bank dot org or maybe you just take out

41:59

a letter you know and whatever the case is so then you'll get emails that will

42:06

ask you to do something and then they will get access to your stuff transfer

42:10

the funds or have you transfer the funds in a lot of cases and that's how they

42:15

make the money and then a couple months later the actual company that was

42:20

sending you invoices in the first place calls up and says hey we haven't been

42:24

receiving your your payments you guys have been great for the last year but we

42:28

haven't received payments for the last three months we thought maybe it was a

42:30

glitch you know but it's been three months and we got nothing and you guys

42:34

the business say no we we sent payment you say and the business of the the

42:39

contractor the the vendor says no you didn't he said well here's the check

42:43

number or the the transact the transaction number and the business says

42:48

the vendor says that's cool but we still don't get any money say well we sent to

42:54

that new account that you told us to send it to I said we didn't tell you to

42:58

send it to a new account and then it's a real bad day for a lot of folks right so

43:03

big thing to keep in mind always when you get email don't just blindly follow

43:11

words on a screen stop and ask questions call somebody ask the CEO or call the

43:19

vendor you know talk to somebody talk to a human being

43:23

that's the best way that I can tell you guys to validate some of this stuff

43:29

because if you call a phone number you know that somebody's asking you to call

43:33

bad guys think this stuff through again right so are they gonna tell you in an

43:38

email to call the actual business or are they gonna tell you to call them so

43:42

what's the answer that you're gonna get use the number that you know how to call

43:46

in contact folks we are all perfectly capable of googling stuff today right I

43:51

think that's not a surprise look it up take five minutes to validate and verify

43:57

so there's some examples of commercial account takeover we had some really good

44:01

examples we've talked about business email compromise same thing who here

44:06

uses office 365 awesome keep your hands up real quick

44:11

nice and high now for those of you guys putting your

44:15

hands up who's got multi-factor authentication turn on do it go home do

44:20

it right now like first thing for real use multi-factor authentication on

44:26

everything that you can because what did I just talk about when we talked about

44:31

these password things right where were we at bad guys know this stuff office

44:38

365 is extremely susceptible if you have an email and a password that's ever been

44:48

compromised and you're using the same email and password for office 365 maybe

44:53

you don't even know it's been compromised right multi-factor

44:57

authentication effectively blocks like 99% of online what we call either

45:03

password reuse or password spray attacks remember we talked about bad guys just

45:07

load this stuff up in a program and they just go log into stuff

45:11

office 365 especially we've dealt with four or five office 365 account

45:18

takeovers just in the last few months that would have been mitigated by simply

45:22

turning on multi-factor authentication you guys know what multi-factor

45:26

authentication is right and there's multiple ways to do it text messages

45:30

email verification which is not the most ideal if you're getting email

45:34

verification to log into your email right but text message and there's also

45:39

the Microsoft Authenticator app so if you got a smart phone you can just hit a

45:44

button right but for a bad guy then to access your email account and whatever

45:50

else you guys utilize under office 365 like we have our entire infrastructure

45:56

in office 365 right now you know we don't have we've gone serverless at SPS

46:02

when it comes to our files and our stuff right so we don't have a file server we

46:06

don't necessarily have we're working to move away our domain controller but you

46:10

know so we've got two factor authentication in a lot of different

46:15

places when it comes to office 365 but if bad guys want to take over your

46:22

email not only do they have to just get you to

46:24

click on something they've also got to compromise your phone and you use your

46:31

credentials that way make sense use two-factor multi-factor authentication

46:36

on everything that you can if you take nothing else away from this that will

46:41

help but when it comes to email compromise that's that's what we see a

46:50

lot interestingly you know the most recent email compromise was from a

46:57

banking association that called us up and said hey we just got word from all

47:03

of the banks in our membership that they're receiving strange emails from us

47:07

with malicious software and links we didn't send them out at least we don't

47:12

think we did so can you dig in and help us find it

47:15

out they used office 365 their managed service provider left the online access

47:20

portion of it on but didn't tell the bank or didn't tell the association so

47:27

they didn't even know when we called them and I said hey can you log in from

47:30

home you know can you log into office 365 or you know your productivity suite

47:34

from your home computer no I don't think we can do that I think we could only do

47:38

that from our our place well that's kind of what office 365 is about you know

47:42

being able to get access to your stuff anywhere anytime you can you turn it off

47:47

externally yeah you can do that but double check and make sure they sit we

47:53

got a phone call about 10 minutes later oh crap

47:56

you know we totally can well that's how bad guys got in they used a email and a

48:03

password that was been compromised somewhere else probably right so

48:08

important stuff all right so what is Blackhawk doing to combat cyber threats

48:14

a lot of stuff so external penetration testing unfortunately it's a little bit

48:22

less this in terms of external penetration testing and a little bit

48:26

more this you know which is a lot more boring than hackers the movie but you

48:33

know you know my network security guys made me put

48:36

in there but external penetration testing attacks your the the network

48:43

devices that are connected to the Internet as a hacker would right so it's

48:49

scanning it's looking for open stuff and it's seeing what's exploitable and if

48:53

there's some stuff that's exploitable you know it would see if we can get in

48:58

so that's kind of what an external penetration test does if you're Boris

49:02

the Ukrainian hacker dude this is the process that he would use to scan your

49:06

network and see if he can get in through the firewall or see if you've got you

49:10

know a Windows XP box on your network that's talking to the Internet okay

49:16

they do phishing email testing anybody here ever heard of no before

49:20

awesome you guys use no before super cool we talked about people being a big

49:26

risk and phishing being bad guys number one you know vehicle of choice when it

49:34

comes to hacking stuff know before is a phishing email simulator and it's pretty

49:42

cheap all things considered and it allows you to test your employees it'll

49:46

send phishing emails to folks that aren't malicious but operate in the same

49:52

way that a real phishing email would and then there's a lot of training and

49:55

education that goes on on the back end if they do click on stuff then they get

49:59

an email or a notification and say hey you clicked on a phishing email and now

50:03

you got to take this 15 minute training as to what's going on anybody here ever

50:07

taken know before training and all the blackout folks are raising their hands

50:13

that's awesome it's a pain in the butt it really is but it's effective because

50:19

you can't just watch a 15 minute video in the background and go do something

50:23

else cuz you have to interact with it you got to click on stuff you know it

50:27

asks you to participate so it's good it's good training that way but really a

50:32

cool thing to do and I'll let Jess and Sarah talk a little bit more about this

50:39

afterwards but they've also got this list of things and that not only they do

50:42

but they offer to you guys in terms of protections for you know business online

50:48

commercial online banking you know we talked about multi-factor

50:51

authentication set it up guys you know positive pay monitoring of transactions

50:57

strong passwords and periodic changes I know that nobody likes to change their

51:03

online banking password but again you know we talked about password reuse it's

51:07

important for that reason dual controls this type of education building strong

51:14

relationships and that's kind of segue into our next slide here is you know

51:19

what do you what can you do to help well we're gonna talk about the ten things

51:22

real quick but also just make sure that you got a good relationship with your

51:25

bank all right talk to them the better they understand what you guys do and

51:30

what you do on a normal basis in terms of transactions the better they can help

51:35

identify anomalies and when your bank calls you up and says hey we're just

51:39

verifying that you really want to do this don't take it as them being a

51:44

roadblock take it as them looking out so you don't wire a hundred thousand

51:49

dollars to China and never get it back right so and if they call you and they

51:55

say hey we think that this is a really bad idea

51:58

it's probably a really bad idea okay so talk to your employees as well and then

52:06

check out some of these additional security things so we've based this on

52:11

it's a little bit older of a standard the standards been updated but I still

52:15

like it as as being really relevant to small businesses because we're talking

52:21

about the absolutely necessary things that every business and for the most

52:26

part you know people at home need to do today as well so here are the 10 things

52:32

number one good anti-malware now there are two different types of anti-malware

52:39

that you can use today there is behavioral based anti-malware and

52:44

signature based anti-malware signature based is kind of your traditional

52:49

antivirus that's typically what you're gonna see when you use free antivirus

52:52

and again it's better than nothing you know but it's not as good as behavioral

52:57

because signature based antivirus it has to know that something is bad before I

53:02

can block it but most malware today changes itself

53:07

every time its installed so if you got 30 different computers on your network

53:11

and it might catch the first one but if it installs itself the second time it's

53:18

going to be a different piece of software or at least it's gonna identify

53:22

as a different piece of software based on what we call the hash right so if

53:28

your antivirus if its signature based might only block one thing and it might

53:33

spread around behavioral based actually analyzes the code of malware and it says

53:38

hey what's this thing trying to do so it analyzes it it kind of runs through and

53:43

it says ah this is gonna be bad stuff we're not gonna let this run okay so but

53:49

some antivirus is better than none antivirus so keep that in mind

53:53

hardware firewall make sure that you've got a good hardware firewall if you were

53:58

a business make sure that you've got a commercial grade hardware firewall not

54:03

just one of those Linksys Wi-Fi router firewall combos that you can pick up at

54:08

Best Buy and again that's better than nothing but it's not gonna be as

54:14

effective in today's environment as a commercial-grade

54:17

firewall so but again you know your firewall you know here's all the bad

54:23

stuff out on the internet here's your internal network that's what the

54:27

firewall is meant to do is keep all of that stuff out similar concept to a

54:31

hardware firewall is a software firewall and it's a little different today but

54:36

you guys you know that have used computers for the last 20 years know

54:40

that you know you buy a new Windows computer and the first thing that you do

54:44

is go turn off Windows Firewall cuz it's annoying you all the time and asking you

54:48

if you want to really do this or you know maybe we you know need to block

54:53

that but don't turn that don't turn that off that provides an additional layer of

54:59

protection on each device that you have on your network a lot of antivirus

55:05

companies now have have moved away from simply being an anti-virus program to

55:10

what we call endpoint security so a lot of times it's it functions as a software

55:16

firewall in it a virus and it does some email security

55:19

and in some of those things those things are absolutely worth paying for guys

55:24

right you know it it's okay to pay 30 bucks a year for a license of antivirus

55:32

or whatever it cost 2,000 bucks for a commercial version or whatever the case

55:36

is right it's gonna be worth it from a security perspective software patching

55:41

who here has a formal software patch program at your organization kind of

55:48

sorta maybe right remember what we talked about earlier when we're talking

55:52

about Windows XP and Windows 7 hitting end-of-life right and and the

55:57

reason that that's important is because software patches protect against

56:02

vulnerabilities if you're not patching effectively then you're leaving your

56:07

organization very susceptible to when somebody does click on something bad

56:14

guys are just gonna have a field day right so if you are at least doing basic

56:19

patch management on some Ford sort of schedule and somebody's paying attention

56:24

to it and not just Windows stuff too but browsers Firefox and Chrome Microsoft

56:31

Office Adobe Java a lot of these other things all have known exploits so in

56:41

fact I was just putting together a different presentation last night and

56:45

out of the top five known exploits three or Windows one is Adobe in one is

56:50

Microsoft Office right so keep those things in mind those are the most

56:54

actively exploited things on the Internet today number five here is

57:00

backup your data if there's it outside of going and turn it on multi-factor

57:04

authentication for anything that you can turn it on back it up your stuff is the

57:08

most critical and even more critical than that make sure that as has been

57:17

mentioned maybe a couple times today that you don't just back up your stuff

57:20

and keep it on the same network because if you get ransomware

57:23

it's just gonna affect everything that's on your encrypt everything that's on

57:27

your network in the first place so make sure that you've got an off-site

57:31

back up we worked with an organization in Kansas City here just a couple months

57:37

ago that had ransomware and they're a aerospace contractor I don't think I'm

57:43

gonna offend anybody here hopefully nobody's working with those guys but

57:48

they're about a 300 million dollar organization they're about five years

57:52

old they do DoD contracts and they do major aerospace manufacturing for up

57:58

five clients here's the list of their five clients the Department of Defense

58:03

Boeing Northrop Grumman Lockheed Martin and Spirit Airlines that's it and they

58:11

had ransomware on their entire network we were able to salvage their most

58:15

recent three days of backup but they backed up they mirrored on their same

58:20

network it was just to a different location but they didn't have an

58:22

off-site backup that was what you would call air gap right an air gap means that

58:28

it's not always connected to your network obviously a backup has to talk

58:31

to your network for a period of time to do a backup but you know think about it

58:35

like plugging in a USB external hard drive back and stuff up and and taking

58:42

it with you home you know that's an example of an air-gap backup you know or

58:47

it could be a cloud-based connection where that connection shuts down or

58:50

whatever the case is but again if if it's connected to your network and you

58:56

get ransomware and your pack ups get encrypted too you might not have a

59:02

business anymore and so if there's nothing else you know

59:06

outside of the multi-factor authentication thing that you guys take

59:09

away from this is have really really really good backups and make sure that

59:14

you've got a copy off-site that's air-gap okay

59:19

number six is physical access security making sure that we're considering

59:25

physical access in the world of hackers physical access is game over if I can

59:32

touch a computer of yours I own it so keep that in mind for customer

59:40

interactions when people come vendors come to your organization when customers

59:44

are wandering you're building right you know keep

59:47

those things in mind but also secure your physical perimeter lock doors have

59:51

cameras you know put digital locks on on doors if you need to whatever the case

59:57

is right all of this stuff is so cheap today that there's really not an excuse

60:01

to have good physical security and then just keep in mind don't let people just

60:05

wander around in your buildings stop ask questions make sure that folks aren't in

60:09

areas that they shouldn't be number seven is wireless security similar

60:15

concept to some other things earlier but you know big picture of things here

60:20

do not use wireless unless you have a business reason to use wireless wireless

60:26

is okay we can secure wireless if you don't need it then don't use it right if

60:30

you don't need to offer free public Wi-Fi in your organization's but don't

60:34

do that either if you want to do that then make sure it is a completely

60:39

separate network then your business stuff because if you have it all on the

60:44

same network and I log in or or access your Wi-Fi and I go looking around and

60:51

you're all of your business stuff is on the same Wi-Fi guess what I'm gonna find

60:56

stuff and you don't want me to find so from a customer perspective so make sure

61:01

that it's set up securely turn on wpa2 at least wpa2 use a strong password you

61:11

know spring 2019 not a strong password talk about that here in a minute

61:16

understand that there are security vulnerabilities in wireless technologies

61:20

they also require firmware updates right again there's risk here you know when we

61:27

go back to patch management patch make sure that you're checking for patches

61:31

and updates and and whatnot for your firewalls and other network devices

61:35

including wireless access devices as well so lots of things to keep in mind

61:41

there but use use passwords make sure that they are long and complex you know

61:46

you should really only have to enter them one time for the devices that you

61:50

need them to use or to access Wireless so long and complex that way they can't

61:56

it's harder to crack secure restraining that's why you guys are here

62:01

today to learn a little bit more about this take this information share it with

62:04

your folks you know I know at least a couple people have asked for the

62:08

presentation I'm sure we're happy to share that out and we've got the

62:12

recording you know you share this with your folks otherwise ask questions you

62:17

know my contact information is up here you got Sarah and Jessica that are gonna

62:21

come up here and talk a little bit more you know use us as resources even if you

62:25

have questions if you think somebody clicked on something you feel free to

62:29

call us you know we can check it out an email pretty quickly we talked about you

62:35

know phishing being bad guys number one vehicle but remember phishing is an

62:40

insider threat if I'm Boris Ukranian hacker dude I can send out two hundred

62:45

thousand emails if nobody clicks on anything I'm dead in the water what has

62:51

to happen for my phishing email to be effective somebody's got to take the

62:58

bait meaning what when I click on something right where is that person

63:02

clicking on it from outside of your network or inside your network

63:06

exactly right phishing is an insider thing somebody's got to let a bad guy in

63:11

it's it's not it's the fault of the phishing emails but that's that's part

63:16

of the cause you know the effect is is us clicking right so keep that in mind

63:21

unique user access controls make sure that users all of your users are not

63:26

administrators on their own devices that's a real bad way to let bad guys

63:32

have all the access that they want on your networks if they do get in segments

63:38

some stuff off and then we talk about passwords make sure to use good

63:42

passwords right spring 2016 or 19 or whatever it is you know an average

63:48

computer can crack that in seconds today with cloud computing and GPU cracking

63:58

boxes as an example at our office we have and if you guys know what a GPU is

64:03

it's a graphical processor it runs video and stuff like that so they're really

64:09

powerful and we've built a GP you cracking box with eight different

64:16

GPUs in it that have 16 gigs of ram in them each it churns through passwords

64:21

you know against our password lists in no time flat we can crack 12 character

64:28

passwords in about 5 minutes if they are not overly complex so keep that in mind

64:35

and then there's cloud processing that you can use this through to so for

64:43

example you know today even though this is a longer password

64:48

you know that's 1 2 3 4 5 6 7 8 9 10 11 gocubs 2019 exclamation point not really

64:58

considered that strong of a password today we want links this is where we say

65:03

you know 12 14 16 character passwords people you know have different methods

65:09

to do that you know string for random words together I just like sentences you

65:15

can use it sentences password find a quote or a song lyric or something that

65:18

you can remember and just type it out spaces and caps and punctuation and

65:22

apostrophes and whatnot you know so hey Chicago what do you say Cubs are gonna

65:27

win today it might take you five seconds to type that out you doesn't have to be

65:32

the whole thing either you know but that's that is an extremely strong

65:35

password today and one thing you can remember if your Cubs fan so also limit

65:43

access to data make sure that not everybody gets access to all the same

65:47

stuff that your internal network is wide open you know everybody can see

65:51

everything limit it down to the principle of least privilege right if

65:55

you don't need access don't give people access so those are the top 10 things

66:01

we've got there are some other cyber security frameworks that if you guys

66:06

want to move beyond the ten basic things there's some other things that you guys

66:12

can go check out this is kind of you know where we live and what we do so if

66:16

you guys have any questions on what this stuff means or how you go about doing it

66:20

please let us know and I'm going to finish up here with just kind of this

66:25

security lifecycle right we started today about talking about risk

66:30

and this is this is really what we do isn't as an organization SPS we really

66:38

want to help folks understand risk and before you understand risk you have to

66:41

know what you have right you know what you have you figure out what the risk is

66:46

and then how you want to handle that risk so you assess risk and you assess

66:50

risk not to just know what the risk is put the make good decisions on how we

66:54

mitigate that risk you know you're not gonna go home and do all ten of these

66:57

things tomorrow right if you do awesome but typically they take time it takes

67:03

time to do this but you gotta be able to prioritize some of these things but you

67:08

assess risk to make decisions on what controls you're gonna put in place you

67:12

implement controls and then you want to test them right we talked about people

67:16

process and technology that's how we test security stuff - right so we test

67:21

your processes your documentation you know we do IT audits for financial

67:26

institutions as an example you know are you doing what you say you're doing to

67:29

protect stuff and is it enough we do technical testing the vulnerability

67:33

assessments and the penetration test we test people through social engineering

67:37

phishing emails physical impersonation dumpster diving a couple other things

67:41

like that and then we go through that testing process we come up with some

67:45

findings and recommendations on how we get better what we should do next and

67:49

then we start all over again that's how we improve so that's kind of what the

67:53

security lifecycle looks like if you you take away from that and it's the

67:57

plan-do-check-act methodology so but you know quick

68:04

summary here Security's everybody's responsibility affects everybody today

68:07

there's no such thing as we're a small business in the middle of nowhere and

68:11

nobody can find us we don't have anything of value right remember those

68:14

are just myths it's not true you have stuff of value bad guys can find you

68:19

you're just number on the internet and it's all automated so take steps to

68:24

secure your stuff your networks your financial data continue to work with

68:28

your bank if you if there is anything suspicious call somebody you know I'm

68:34

Jessica and Sarah will be more than happy to either help how they can or

68:38

direct you to somebody that can help same with me so if you guys need some

68:45

assistance please reach out or you see some suspicious but you know one of my

68:50

favorite quotes quotes especially when it comes to information and

68:54

cybersecurity is we've got to just think a little bit differently here right we

68:59

can't pretend that it's not our problem today when it clearly is and there are

69:03

more data breaches and more stuff being hacked and more folks losing money and

69:07

more identity theft than there ever has been and it continues to increase so if

69:11

we just change our thinking a little bit and say hey you know what this is really

69:15

important you know then things will operate a little bit differently your

69:19

organization

English