What Small Businesses need to know about Cybersecuity

Thank you everybody for joining us today I am excited to bring this information to you. My colleagues and I are going to try to give you a lot of information on how to protect your businesses against cyber threats. I will be covering a little bit about the awareness and wrists in today's complex trust, threats, Ryan will talk about protecting your business, response recovery, and Mitchell will come up with helpful resources tour you.Trend Micro try to educate organization , organizations about threats that are affecting you today, could affect you in the future, and how to protect your businesses from the cyber threats. I have been in the industry for over 23 years now, all with Trend Micro and it is been interesting to watch the shifting tides that make up the cyber security industry. Our CEO, has talked about our competitors. We do not look at our peers as our competitors we look at the cyber criminals, hackers, is our competitors and those of the people we are trying to deal with to help protect your organizations that we have been in the business for over 30 years and we have seen these things, looking for ways to protect.

>> The first thing I want to highlight about the whole awareness, IBM recently published some information about data breaches that they have analyzed over the course of the last year. One of the things they noticed is small businesses have a disproportionately larger costs then are relative than their peers in the industry. When you look at large enterprises, when a data breach occurs, it is about $204 per employee. When you break it down to small businesses it is a little over 35 employees. Small business owners have to support the brunt of the costs and it can affect your organization much more than it can affect a very large organization.

>> The other item they mentioned was the lifecycle of the data breach in 2019. Up to 279 days that are breach has been inside an organization, actors are inside an organization, from the time they penetrate your organization to when they are able to actually excrow traded and taken off the network is about 279 days. That is a significant amount of time to actually have a actor inside your network doing potential damage of your systems. We also publish, every six months we publish the cyber risk index. This is a survey we do in the U. S. to organizations from small business all the way up to large enterprises. We look at, we take the how you are doing protecting your organization from the threats and compare it with the actual threat landscape of today's - today. We do it index where we do subtraction. You can see here the overall small businesses have a higher cyber risk index from medium business or enterprise which are in a positive, all of these are in the elevated cyber security risks today though. A couple of things, when we highlight some of the areas we look at in the cyber risk index. For example there is superstructure ricks, human capital risk, operational risk, when we look at some of the top items in the area, when we look at threats most organizations are most concerned about Fishel and social engineering threats, click jacking, ransomware is obviously having a big impact again. We saw a decrease last year but we are starting to see the increase. Human capital risk, you need to understand it is a tough - tough to hire cyber security professional, professionals. The cost is high so organizations are having a difficult time there and the infrastructure side, when you think about the elevated risk tied to operational, there is lost revenue, disruption of your infrastructure, and lack of intellectual property, etc. There is a lot of wrists associated with cyber attacks is an organization that you can find this by the way, you can take your own assessment if you go to Trend Micro /cyber risk. One of the questions we ask the likelihood of a successful cyber attack in the last 12 months, unfortunately 80 % of the respondents said it was likely or very likely that they would experience a successful cyber ISAT, attack. One of the reasons we are doing this webinar is trying to prepare you and help you with defending against those types of attacks that

>> Let's shift now and talk about today's threats. I will highlight to that we think are very critical, to small businesses today. Those are ransomware and business email compromise. I will talk about each of these. This will be an overview there's a lot more information on our website to give you information about these two significant threats. As I mentioned, you can see on the left-hand side, this is the overall ransomware count, these are detections across our customer base, we have 5000 - 500,000 customers around the globe that we help protect against dot in 2016 was a big year of ransomware where we had over 1 billion threat, threats block for our customers dot in the first half of 2019 you can see we almost hit the total number from 2018 so we are seeing a resurgence of ransomware targeting small businesses and other businesses around the world.

>> The other thing you can see here on the right-hand side are new ransomware families. These are new families of malware, ransomware that criminals are creating. You can see here that that has been dropping significantly. One of the reasons is because we have seen a transition in the ransomware attack process and the malicious actors are targeting organizations that one of the big things they are doing today is looking at the attack surface against your organization. There obviously seeing you are using more devices, IOT devices, mobile devices inside your organization and they are looking to attack those types of systems to give them access to your organization.

>> The other area, this is probably the bigger piece, they are being much more targeted in their approach. They are now looking at organizations and finding organizations that they want to target, they are identifying the critical business systems inside your organization that if they were to target those and take those down, it can disrupt your organization - organizations business. These could be systems that are critical to running your business and if they take those off-line, they are much more likely to get you to actually pay a ransom. They are more likely to pay a higher ransom as you have seen in the news over the last several months, a number of municipalities, educational sites have been hit and they have actually paid significantly high ransoms to unlock their systems that the good news is we see the U. S. governors come together and vowed to not pay ransoms. Obviously if nobody paid a ransom, this threat will probably go away because it is based on the ability of people to pay the ransom and if we got everybody to stop paying it would likely go away.

>> Another aspect of it is they are building more invasion techniques. While they recognize the security industry has come up with some clever technologies like machine learning, artificial intelligence, behavioral monitoring that allows us to detect ransomware more in real time, as such they needed to build better evasion techniques we are seeing more absolute location, technique built into the ransomware, malware itself. They are using legitimate software in many cases to propagate the threat. We saw recently a MSP being utilized as an infection source and allowed the systems that are managed by that organization to get infected. Distribution models is changing. All of these things are being taken into account that has allowed the ransomware actors to actually increase their ability to infect organizations more effectively as well as command a higher ransom when they do infect organizations that

>> When you look at the industries that are being affected, you have probably have seen this in the news, you can see the top three our government, healthcare and manufacturing. Again, these are industries where if you can take down a critical system that runs the operations of these organizations, the likelihood that they are going to have to quickly remediate and get the systems back online. Criminals are hoping that means paying the ransom. As such, if you are in these types of industries, you want to take extra precaution because you will be targeted by ransom where - ransomware actors.

>> We look at the future, I mentioned IOT, people are not going to pay a $1000 ransom for device which takes $100 to replace that what you will probably start seeing is the industrial IOT infrastructure being targeted. These are the robots, cameras, security cameras, things like that that they can target that again our business operational systems that organizations use and that is who they will target.

>> I want to switch to business email compromise. This is a threat that obviously it has been targeting organizations around the world for some years. In July you see, they sent an advisory out, the United States treasury organization that sent this out. You can see here the criminals over 9 billion and possible losses affecting U. S. financial institutions since 2016 that the threat is real and it is causing disruption. When we look at our data in 2018 from 2017, definitely an increase. The numbers are not very big and that is because business email compromise is a very targeted threat. For the actors behind it, they would do a lot of due diligence to identify which organizations they want to target, how they want to target them, there is a lot more involved in launching it this email compromise attack then ransomware which tends to be more broadly based.

>> When you look at the sequence here, with business email compromise, the big thing is the actors behind it is working on socially engineered email that have legitimate apparent. Typically you will have some executive [ Indiscernible ], they will target the owner, AVP, the executive inside the organization and have an email sent with some sense of urgency, a request for action and some financial implication that typically what we are looking at here is them requesting a transfer of funds, that allows the criminals to get money from the organization. Emails usually at the forefront of this so they will send an email either from a compromised accounts inside your organization or from an account outside the organization that has been spoofed to look like your organization.

>> Some of the things we see when we are looking at a email message itself, some of the attributes of a phishing email. The from field usually will be some kind of spoofed data. They will spoofed the executive inside the organization that the email messages coming from will be either a compromise account inside the organization or come from a free webmail service, outside service or a domain that has been created to look similar to your domain. The date and time will be a very relevant, usually they will send it during business hours so it could be part of the clunker people get in their email so they probably won't be looking at it more critically if it had been sent off hours. The subject line will usually have something they are familiar with. If it is financially motivated, it may have financial messaging inside this subject line. It could be if they are trying to get access to the users accounts, you may have something of interest to them. The body is very short, usually has a sense of urgency listed inside of it. In some cases it may have an attachment, it may not, it may have a link or attachment but in many cases with CEO fraud type emails, there is no attachment, there is no link inside it just tries to get somebody to do something that they normally would do on their day-to-day jobs, transferring funds to a supplier or something like that.

>> When you look at the CEO fraud, we are seeing a lot of against office 365 customers. If your organization has migrated to office 365 or you plan to move, understand they are definitely targeting those organizations. What you are seeing is a pop-up account request, the email message may contain an attachment or link but they ultimately, the user will see a pop-up that looks similar to the office 365. Why they are doing this is to get the credentials from the users for that account so they can take over the users email account and start sending their own emails inside the organization. Some of the recent tactics we have seen - shifting from the CEO fraud to direct deposit. They are sending it to HR and requesting a change in the pay check for direct deposit for an employee. The email will look like it comes from the employee to the HR director saying I moved or changed banks and I need you to change my direct deposit to go to this account instead of my old account. Be aware of that that is one tactic make sure your HR people are aware of this. This email is one that was used inside of Trend Micro. They spoofed a internal micro employee to one of our HR directors and try to get them to change. They are moving down in the employee levels that one of the predictions we have made this year was that they moved down in the organizational chart. We are seeing that. This is an email sent to an employee from a mid-level manager where they requested the employee to do a online transfer for some funds and they would pay them back.

>> Another one we are seeing is give cards, they are becoming bigger and bigger now where they request the gift car, an employee to purchase the gift card and send in the information so they can unlock and utilize the gift card. They are sending those directly to employees inside the organization. When we look at the data, there are two things that are typically used in business email compromise. Positions that are impersonated, a chief executive, number one managing director, president, general manager, in the executive area again. Who they are targeting inside the organization when they send these, again mostly financial right now, the accountant, comptroller, accountant, etc. comptroller, accountant, etc. The majority is still trying to get you to wire transfer funds from your account to their account.

>> I want to shift a little bit, that is all I had today so I was shifted over to Ryan who will talk to you about protecting your business. Thank you very much.

>>Thanks Jon, thanks everybody for joining that was good information . As a reminder will have a Q&A session at the and for any questions. I was shift gears from Jon's conversation and we will talk about advice for protecting your own business. A lot of this advice and recommendations are - you may be familiar with a ready. I will not focus heavily on Trend Micro or our products and solutions this is intended to provide you guys some good information to help protect your business and make decisions for yourself. If you have any Trend Micro specific questions , questions about our products, we will be happy to address those at the end of the presentation.

>> The reason for what we are talking about today is attackers out there pray upon numerous things like human error, that is probably the biggest vulnerability we see today. IT security complacency and this is particularly relevant to small businesses who may not even have an IT person. You might be just picking the one person in your office that knows the most about computers and making them the de facto guy. Technical deficiencies which is related. What I will cover today is a couple of recommendations into different areas. The first area will be on the human side of it, the user side, what can we do from the people perspective to help improve the security of your business and I will talk a little bit about some recommendations on the technical or computer, or device side of it and things you need to think about, work with either your IT person, the person acting like your IT person, if you happen to use a service provider or outside company to do your IT work for you, these might be good things to discuss with them.

>> Some best practice on the user side fall into four different areas. Some might seem obvious but we talked to many businesses every single day, we analyzed billions and billions of threats, and a lot of these things would not exist if some of the basic principles are followed. While they might seem obvious everybody is not doing a good job, passwords of course first and foremost. We highly encourage and recommend different passwords for different accounts. Of course that can become a burden so we use the password, make your passwords hard to guess, do not write the password down and stick it on your keyboard or under your desk that I see this all the time when I've visited businesses that it is common to see a posted under keyboard, cabinet drawer, desk drawer, etc., do not do that. Do not tell anyone your password. The significance of all of this is not to make this difficult for you to remember passwords, the significance here and how it ties back to what Jon share, most people who use the same password for everything including their bank accounts . If your password gets into the hands of a hacker, and it is stolen from it insignificant site, they will take your password and try to use of that banking site the financial institutions. They will get access to your money. Especially in businesses where a lot of business bank accounts may not provide the protection if your money gets stolen that in personal accounts a lot of banks will cover that but often times this is accounts do not have the same level of security.

>> I often see in organizations a lot of people will use the same password, they were use the same password to get into work related systems but is important to change those. Email safety, Jon cover these. This probably the number one way threats enter a organization today especially when it comes to phishing. We recommend of course people invest in phishing awareness training for you and your employees. I say invest, it does not always cost money , Trend Micro offers a solution , we do not charge for that and their other companies that offer solutions as well. Many will offer their services for free for smaller customers, 5 or 10 employees. The waste these work - the way these work you can set up a fake phishing campaign and see which users click on things, their training videos, some awareness opportunities to educate them on how to identify phishing emails, what not to click on, etc. that I heavily recommend getting phishing training in general for you and your employee because this is the number one way that threats are sent today.

>> Many of the business email compromise scams that Jon mentioned, the CEO fraud, the phishing scams, they all start his email, this is probably the number one area to focus on. Terms of online safety, I have seen a few questions pop up, using two factor authentication is a huge thing you should be doing today that what that is, you have probably seen it, whenever you sign into a website or some application and it sends a text to your phone with the code, and you have to put that in as well, that is an example of two factor authentication. It is having a two pieces of information to allow you to log into something that one is something you know, and one is something you have which will be your phone. It is important to really utilize what that - utilize that wherever you can. Many applications like office 365, Google has it, they may not all call it that but that is what it is, look for two factor authentication or multifactor authentication or login authentication. Whatever they call it is important to utilize that.

>> In terms of links, trust and verify. Don't just click on any link, do not assume it is secure because it looks like it came from a trusted friend. That could be a hacker pretending to be one of your friends and sending you links. There are simple ways you can mouse over a link to see if it matches what the link says or you could go to the links directly, if it looks like I email coming from your bank, instead of clicking the link, open your browser and go to the bank website and see if it is legitimate or not. Minimizing use of the cloud file sharing tool. These are great tools, really productive, easy to share and so people that way but they also generally do not provide security. It is easy for a bag guide to upload a bad file and send the link around and spread that way. There are tools, that can provide virus scanning and file scanning within these environments. If you are heavy user of these types of tools in your business, that might be something you want to look at investing in to provide security. Don't over share online. A lot of what we see, a lot of threats now are perpetrated via social engineering. What happens is, hackers will, they will find you on LinkedIn, Facebook, things like that, a lot of people are guilty of putting a little bit too much, over sharing on the platform, your birthday or things like that. It is not uncommon for hackers to go to a bank, click on the forgot password link, it asks you questions where do you go to high school, what year you were born, your favor pets name, stuff like that, believe it or not a lot of the information can be found online if you search hard enough and there are tools to hackers used to scrape that information. Just be important about what you are sharing online and who you are sharing it with especially on the social media side.

>> Outside the office being cautious of public Wi-Fi. It is great to go to Starbucks and pop online but just because it looks like a hot spot or some other businesses hotspot doesn't mean it is. It could be a hacker setting up a fake hotspot and now you are connecting to theirs, me while they are capturing your information. Pay attention to what you are connecting to. You might see someone might have a hotspot that looks almost the same, it will be a Starbucks with a at the end of it. Just make sure you pay attention to what you are connecting to. Keeping your private were conversations private of course and the last one restricting remote access. This is a big problem we are seeing today related to ransomware. Most people, some people have a ability for you to work from home so you connect in from home into your office and access your files and things like that. The way it is facilitated is through technology call our - REP. They don't have an IT person, hackers can get in that way and a lot of times they will scan the Internet for the open ports, they will find your particular server is open and accessible, they will be a boot force attack, they take all the passwords and they will keep trying every combination to get in. Eventually they are successful in many cases. A lot of times again people read, use the same password, or predictable name, it's easy for hackers to figure out and get in. Restricting remote access, putting a VPN in front of that server, put VPN first as an additional layer of protection.

>> Lots of recommendations. There is not a comprehensive list but these are some of the big recommendations and things that makes the biggest impact in improving security. On the device side, generally speaking most instances have these types of devices. From a computer and server standpoint, the first and foremost we recommend, we advocate protecting every device. Putting a antivirus security on every computer in your network, every desktop, laptop, server, even computers people might bring from home. Usually rip we recommend you do not allow that, or a guest wireless network. Or airport where they are not [ Indiscernible - low volume ] they cannot access your servers and things like that. You want to install a managed business grade solution. I point that out because you could, typically we see people, they can go to Costco and buy a copy of something, a consumer product cheaper, but you use - lose a lot of function. If you cannot essentially manage it, you cannot enforce security policy across all your devices, you do not get alerting and login so you don't know if there is a problem in one area before it spreads. Have a good business grade security solution. We sell one in many companies sell good products that can address this requirement.

>> Isolating payment systems. This should be a obvious one if you are a business that accepts payments, credit cards things like that. Keeping your payment system separate from the rest of your organization as best as possible is a good recommendation. Everyone on the call was probably affected by, a perfect example where this was not done, by the target hack a number of years ago, I multiple credit cards, that was a perfect example where the payment system was not isolated, hackers got on and they were able to swipe credit card information for 150 million people. Restricting access to service - servers. Where you store things. You should physically restrict access to the servers, keeping them in a locked room in a server closet, network cabinet, etc. If someone has physical access of course they can get on there with the M-drive and still stuff. Not that any of you would hire people that would do that but it does happen. Restricting network access to servers. Not everybody needs access to everything on a server so you can use - there are permissions that allow you to configure who has access to what. A getting two factor authentication and updating software and firmware regularly. The last two you will see repeatedly. I huge problem that people are not doing, they are updating the software and firmware regularly, these are important. As manufacturers discover bugs and security holes they will release fixes for those. That is why we see a lot of threats, the ones you see in the news, those generally are a result of a lot of systems across the country being out of date meaning they do not have the latest version of software firmware so the threats are allowed to spread.

>> On your mobile devices, phones, tablets, portable barcode readers, you want to enforce passwords and passcodes. This is something your organization may or may not do but millions of smart phones gets lost all the time. If you are accessing corporate information on your phone, like your email, files and things like that and you not password protecting on your phone you are making it easy for people to steal your information. The phone is a great conduit into your corporate data, it is important to protect your phone as your computer and service. Keeping the software up-to-date and installing additional security software. Apple iOS devices, it is not feasible, Apple does not facilitate installing security but android devices definitely do. You do not hear about it a lot in the news but we have a team that turn micro where we see tens and thousands of threads on mobile devices. It is a bigger problem in Asia but it certainly is a problem and vulnerability. As best as possible install security on your mobile devices. Update software/firmware regularly. Another area where people overlook is your networking gear, your Wi-Fi. You might have a Wi-Fi router so you can connect wirelessly. What we see a lot of his people buy these things and plug them in and never change the default username and password. You can go on Google and search in about two seconds and find the default user for any device. You will find it in two seconds. Hackers know this and because the devices are connected to the Internet it is easy to sweep the Internet. There are search engines for doing this, you can find those devices and try to log at. Once you connected it is easy to do what you need to do is a hacker to steal the information you want.

>> Along with that, disabling remote management help solve some of that. They have a feature where you can remotely connect with them from outside the office so you can make changes and things like that. You can turn the feature off that it is important to turn it off. If you ever need to access this device to make changes you should do that within the office and that solves that problem that you can restrict access to specific devices that if you are small organizations, you have five computers and five phones that are wireless, you can set it up so only the 10 devices can connect to the wireless device. If you are business that guests come into, a coffee shop, dentist office, you can set up a separate wireless network it is called an SS ID, it is a fancy term to say you have a separate network for guests. Guests would log on to that. You have probably experienced this when you have gone to a restaurant, and you asked them what is the password to get on the network. That is almost always a separate wireless network so you cannot jump into the business network and still information.

>> Enable in Christian but - enable encryption. Do this regularly. Lastly, there are probably other devices, Jon might have mentioned this, the term IOT, Internet of things, it is a fancy way of saying all the other new devices we are seeing out there that are Internet enabled, your ring doorbell, your wireless garage door opener, those are on the consumer side but you have similar things in your office, smart TVs, printers, copiers, a lot of devices are probably on your network that you do not Inc. about because they are not a computer or phone those are entry points for hackers. What makes them riskier is you cannot, they are typically not running when there is a Mac operating system. You cannot install any solution on them so it is important, change your user password, restricting access, updating the firmware and software regularly. Take a inventory of your environment, think about everybody that is - everything that is connecting to your network, and keep those things up-to-date and making them as secure as possible.

>> Like I said it - if you put a new refrigerator in the break room and it has a screen to play videos, that could be entry point for hackers, anything connected to the Internet or network you want to make sure you are doing your due diligence. Unfortunately we see this more often than not, despite everyone's best effort or lack of best efforts, hackers will still get it to some organizations. If that happens, some advice, it is critical, stop the AT Act - attack. This could be unplugging your business from the Internet, stop the connection coming in into you can access what is going on, or turning off different machines. Stop the attack first and foremost. Restoring from backup, this is especially important in light of ransomware. We never advocate for paying the ransom and we are big fans of making sure you have backups and that you are testing the backups regularly, and you follow the three, two, one backup. You have three different copies stored on two different mediums, a tape drive, hard drive, plus a copy in the cloud and you keep one of them off site in the unlikely event maybe there is a fire, or hurricane that shut you down or does damage. It is important to have those backups. While they were historically meant for natural disasters and fires and things like that, they have become more more important in light of ransomware. The ransomware attack happens, they encrypt all of your cell - stuff, if you backup it is easy to restore. Of course bring in experts if necessary. There are a lot of different businesses out there. IT service providers, they go by different names, SPU. There are companies that are experts in IT and some of them specialize in disaster recovery or attack recovery. If you need the help definitely reach out.

>> Everybody anticipated this may happen to you, you should have a documented written recovery plan. Their templates online you can find. It is more like a checklist of what you would do something like this happens, who do I contact, how do I restore my backup, who does what. You should have a disaster recovery plan. You want to execute on that if this happens. If you are in a regulated industry, breach notification requirements. You have probably seen this or have been a recipient of this, but if you - your healthcare information gets stolen, assess the industry you are in and see if there is any breach notification requirements you have to attend to so you do not get in further trouble. While not everybody wants to do this, if a breach or hack happens, there was probably something missing in your organization. It is a good time to evaluate your existing security posture and see if there is any new technologies that you might need to deploy to prevent future attacks that in some cases this is simply a matter of, you might have the right tool in place but it might be out of date. Maybe you are running an old version, so it is important to check that occasionally and try to stay on top of that to prevent future attacks.

>> With that that concludes my section I will turn it back to Mitchell.

>> This is Mitchel Chang from Trend Micro. To wrap up today's presentation, I would like to also provide you some additional resources in the small business community.Trend Micro, our initiative for education, our outreach program currently for helping the community to have a higher level of awareness and educating the community, we have a Internet safety program helping the K-12 and also small business to better protect themselves. Some of our partners SCORE is one which can help you with Cybersecurity challenges you may be facing. We partner with national cyber security alliance, they have ongoing workshops and webinars as well for the small business. Often times we found small businesses are actually more vulnerable than the large enterprise because you do not have the funding or resources like large enterprises to protect themselves. There's a new organization named the cybercrime support network. They are in another nonprofit group trying to start a 211 service line in the United States for small businesses. Several states are in the process of adopting the 211. Several states are in the process of adopting the 2111 of the channels for small business cybercrime. [ Inaudible - static ] Rhode Island always, already has this. The national Institute of standards and technology, we are sponsoring the ninth conference, the national Institute for Cybersecurity education and we work with U. S. Chamber of Commerce. Those are additional resources we believe that can help the community. The government organizations also, law enforcement's - enforcement. The additional information that you need from us, our initiative for education, for the nonprofit side of our company, we try to help our community to better protect themselves. We want a digital world that is free from attack and exposure. With that we hope you enjoyed the session today and we were help to you to protect your business and assets. I would like to give the floor back to Alexa from SCORE.

>> Thank you. We will begin the Q&A portion of this webinar that we would do our best to address as many questions as possible in the time remaining that we typically have more questions asked in time allows us to answer. If we do not get a chance to address your question in this live segment, I would encourage you to connect with your SCORE mentor after today's webinar who can assist you further with applying these strategies. We will also be sending you the slide deck with the resources that were provided as well so you can reach out for additional assistance and reference those that with that let's go ahead and jump into the questions.

>> The first questions from Deva who is asking, why would cyber criminals target small businesses? It seems more revenue would come from larger enterprises?

>>This is Jon that is a great question and one I get regularly from small business owners. The reality, think about this, the cyber criminals out there they are scanning the Internet for IP's, they do not care who the IP belongs to dot they scan it to identify is this something I can identify. They do not care about finding you. With that said, once they identify you, they can think about does it make sense for me to target this organization. With small businesses there are a few reasons why they will target you. 1st is they will look to see if you are part of a supply chain of a larger business, island hop in - island hop in - hopping. This happen with target. They may target you to get access to the larger organization that you should be looking at any links you have to outside organizations and make sure they are secure. The second thing is people have to understand it is not always about stealing data or dropping ransomware, they may be looking to use your resources, your system to launch attacks against others. They made be looking, they may encrypt a line, they do not want to buy their own systems to do it so they leverage that. They may use your systems [ Indiscernible - low volume ] against other organizations. Think about your systems not as a potential target for data that, daft but as a resource to launch other attacks outside the system. Those are probably the two or three key things of why they would target you.

>> The next question comes to us from James asking where do you get the most bang for your buck with protecting cyber assets? Do you recommend an 8020 rule, what advice do you have?

>> Good question. This is Ryan. The reality is, you kinda have to sure up everything. If you think of it like a house, if you put the best lock on your front door and three deadbolts and things like that but you leave your back door wide open, there still an entry point. I would say at a minimum we typically would recommend, you want to put some type of detection on each device that is connected to your network which is a centrally managed business grade security solution. You want to also protect your email. The reality is today, 94 % of attacks originate via email. Adding additional protection on top of your email will probably give you the best bang for your buck but you definitely want to protect that as well as your other devices. That includes, even if you are using office 365 or G Street, G Sweet, they have a base layer but no advanced threat protection or any sophisticate security technologies that look for phishing attacks . There are vendors out there including Trend Micro that sells solutions to provide additional protection. Even though you are not hosting your own email server anymore but you can still protect your email infrastructure that way even though it is hosted by someone else.

>> From Hilda, she says she is a small this is owner they run a free version of the anti-virus software will that be adequate?

>> Good question. In short, no. A lot of times the free versions, whether home or in a office, it does not matter, you are still a potential victim as Jon explained . Hackers do not discriminate, they look for any resource they can find and they can get in there. Typically, the free solutions out there, you can download free solutions from various companies, they are baselevel functionality. They are okay but ultimately you get what you pay for. Considering how valuable business information typically is, whether that is customer information, names and addresses or more proprietary information, like intellectual property, stuff you have patented or designed, that stuff has value in a free AV solution eventually will provide the type of value you are paying for. I generally do not recommend that. We will recommend that for your typical consumer who might not have that type of important information by for a business I would not recommend using a free AV solution even if his two people in the office.

>> Also I think very key is, most antiviruses are threat defense software from a reputable company provide support and services. That is important. For free one you just get a cheap log but the grade of software stronger and better detection from a reputable vendor, their security attach where you have someone to call is support Center to help you in case you get a breach.

>> We have time for one or two less questions before closing out for the day from Danielle asking if there is a single solution that can help small businesses protect themselves?

>> This is Ryan. Yes and no as I covered in my section. Part of the solution is technical so yes you can buy a solution like Trend Micro worry free business security that if you install on all of your Windows, Mac, android devices, and provide protection on iOS as well, the technical part is only half the solution you also need to shore up the user side. Yes you can buy a solution that will provide a large amount of security but you want to address the user side of it as well. There are areas that one solution will not cover everything. I would say in general yes you can get a good solution that protects most of your devices and you can address the people side of it as well.

>> If we can take one last question before closing and we will be right at 1 PM. From Corey asking in addition to good hygiene such as back up in strong passwords do you recommend any additional recommendations?

>> One of the biggest things you can help is educating your employees and getting them to think about security when they are online. As I mentioned, and Ryan mentioned, let's say they are going through the emails in the morning, they have 50 emails to get through, obviously they are trying to get through those as quickly as possibly but think before you click. That is one of the things that people talk about. Recognize your employees are probably your weakest link so anything you can do to help improve their understanding of how they will be attacked, why, and how, I think will go far for your business and keeping sure you are protected.

>> That was exactly what I was going to say, user education is key. Attending something like this or something similar so they can understand the ramifications of not being more diligent online is a very useful thing.

>>Trend Micro has a ton of resources on a website . A lot of it is video which people like to see. You can go to our YouTube channel and send the links to your employees because there is a lot of content there that helps explain what a threat is, a lot of user education that you can take advantage of for free.

>> The persistency is very important because we see a lot of training happening but a lot of times it is much harder to change people's behavior than just education alone. Dislike drivers of - education, people do not speed but they still speed.

>> Those are all the questions that we have time for in this live session. If we did not get a chance to address your question, again we would encourage you to connect with your SCORE mentor after today's webinar who can address your questions further and assist you in applying these important tips, suggestions and green information shared with us today. As a reminder, a link to the recording of the session and the presentation slide deck will be sent in a post event email. The slide deck contains information. I would like to thank you all for taking the time out of your day to attend the session and I would like to give a big thank you to Jon, Ryan and Mitchell . Thank you so much.

>> Thanks everybody.

>> Registration is now open for the fall startup success conference. This is being hosted by SCORE and FedEx it is a free half-day event being held on October 24 from 12 noon until 5 PM Eastern time. We will have nine education or webinars, one-on-one mentors, networking, and a wealth of resources to help you with the success of you start a business. You can sign up by clicking the link on the slide that is being displayed or by going to the SCORE website at www.dot SCORE the SCORE website at www.dotSCORE.org. Thanks again everyone I hope you have a great rest of the day. Take care.

>> [ Event concluded ]