INSIGHTful DISCUSSIONS

Sponsors' Content Distributed By Greater Wilmington Business Journal

TECHNOLOGY TRENDS FOR 2016

CHRISSY COOR
Regional Manager,
Fluid IT Services

ROBBIE GARNER
President/CEO,
Atlantic Computer Services

MARC MEREYDE
President,
Tiktoplus

SHAUN OLSEN
CEO,
CloudWyze

DEVON SCOTT
Founder,
BlueFission

Advancements in technology play a significant role in how companies set their direction. Successful growth strategies, cost efficiencies and securing data all hinge on making the right technology decisions for your business. Below and on the following pages, five local technology executives offer their insights on recent technology developments and perspective on what to expect in the new year.

What questions should business people ask to ensure their technology investments yield maximum returns and help them grow their businesses?

SHAUN OLSEN: Start by asking these questions:

1. Is my data protected externally, internally and from disaster?

2. Is my foundation solid? IT should be a system, and all systems need a solid foundation. If I'm growing, can my systems handle the growth? Can my IT team get me there?

3. Can my employees access what they need, when they need it and with ease?

4. Do I have a plan? IT strategy and IT infrastructure are two different talent sets. Find that talent and be in the room with them when developing a plan for your company. Revisit annually and when major changes are on the table, and take the time to understand what you have.

5. What are all my options? Talk to multiple providers and ask them to explain what others are telling you. Choose the one that you feel most comfortable with and "gets" your company.

MARC MEREYDE: There are no one-size-fits-all solutions in technology. The newest shiniest technology may not always be the right one for every business. Business people should ask how technology will improve their specific processes by saving time, increasing customer satisfaction, ensuring better business regulations compliance, etc…

Business people should also find out how comfortable their employees or potential customers are with any new technology. There can be no implementation

INSIGHTful DISCUSSIONS

Sponsors' Content Distributed By Greater Wilmington Business Journal

"Most security issues are due to human error by clicking on that one seemingly harmless email or link that exposes the entire company."

CHRISSY COOR
Fluid IT Services

"Should you be the victim of ransomware, do not yield to their demands. Contact your IT professional to clean up your system."

MARC MEREYDE
Tiktoplus

without adoption. If employees and/or customers are not going to use the technology, what's the point? Business people should look at the learning curve and user experience as crucial parts of a good ROI.

Finally, business people should also consider the cost of ownership.

CHRISSY COOR: First they should ask themselves, "What are our business objectives and goals for the next 12 to 24 months?" Maximizing ROI on IT investments requires continual understanding and alignment to the business goals. From there, questions should be geared toward confirmation of the alignment. Is there an IT Roadmap aligned to reach our business goals over the next 12 months? What is the ongoing review process between IT and business stakeholders to ensure alignment?

DEVON SCOTT: The first question should always be "will this technology help take my business where I want it to go?" It's easy to get swept up in current trends and buzzwords and think things like "my business must be in the cloud now to stay relevant." However, before spending several thousand dollars on a new tech investment, ask your provider or IT team some qualifying questions:

1. Does this technology help our business do our job better?
2. Does it solve a problem that we have already identified?
3. Will it allow us to take measurable advantage of an existing opportunity?
4. Will it help future-proof us against an identifiable threat to our business?

Essentially, run the potential investment through a SWOT to find out if it is really helping you. It might seem really cool to deploy a mobile app for employee collaboration until you realize that no technology, no matter how hot it seems (apps, clouds, automation, etc.), is a magic bullet. There might be no worse investment than doing the right thing in the wrong way.

What are the most common mistakes companies make in setting up their technology systems?

MEREYDE: They often forget scalability and security.

SCOTT: Trying to be too hands on with their technology. It can be a curse how available technological tools are. Many businesses will try to implement and configure tools themselves to save costs, but will generally add time to the turn around for implementation and leave many errors and vulnerabilities as a result.

You probably wouldn't tell your office building contractor, "Just give me the blueprint, and we'll install the electrical circuitry." The dangers aren't quite as obvious for technology until you are facing a PCI audit, or your services disconnect 15 times a day, and you can't explain why. My advice is to hire someone to do the technical work so that your company can continue doing what it does best for its bottom line.

COOR: Companies typically do not think of the implications of technology early enough in the business decision-making process. A good rule of thumb is it is never a bad thing or "mistake" to involve IT in business decisions, and it can never be done too early.

Often businesses come to IT with critical needs to implement "tomorrow," only to find out the process will take 30-plus days due to outside factors. This tendency also often means businesses are hyper focused on the "now" rather than a long-term strategy, which can often lead to poor technology decisions.

For example, purchasing a software package that is outgrown in the first 12 months because it does not scale to meet growing business needs. Include IT early and often with a mindset towards long-term strategy.

OLSEN: Companies need to determine their business model, and then ensure their technology supports their business model, rather than drives their business model.

A good example would be an insurance company. The advantages of operating out of a datacenter and focusing on reliable internet service enables mobility, expansion and business continuity. It isn't always "cheaper," but the technology, if implemented properly, can enable the business to grow and take the competitive edge during times of crisis as well as the normal development of their business.

The next mistake we see is undervaluing the importance of technology and deploying it properly versus the piecemeal approach. When working with your provider (whether it is internal or outsourced), you need to get a handle on what you have and how it works.

Don't wait for it to break to understand and don't make assumptions. Ask the "what if's" now rather than later. What happens when the internet goes out? What happens when the power in the office goes out? What can keep us from working? What happens if we double in size or shrink to half our current size?

What should companies think about when exploring options to back up data and disaster recovery plans?

ROBBIE GARNER: Companies should ask themselves a few questions about what their expectations are in the event of a system outage. Can you be down for a day or two? If yes, the simple offsite cloud backup solutions would be perfect. They are inexpensive and reliable. Their downside is that you only have the data backed up. To restore a server, you may have to reinstall the Windows operating system and all of the applications and then start the process of downloading your data. Depending on how much data, that could take days.

Those that could not afford to be down for a long period of time should look to image based backup solutions. Instead of just backing up data, you're able to take snapshots of the whole server throughout the day. These systems keep a copy of the images on a local storage device or server and also transfer a copy to an offsite location.

Should a disaster occur, you could spin up one of your images very quickly. The images are considered hardware independent meaning that they can be brought online using a different server or even a PC. Considering the business impact of your systems being down for an extended time, the cost of these more advanced backup solutions is easily justified.

OLSEN: Backing up data, business continuity and disaster recovery are three separate topics.

Backups are a copy of your data, not the applications used to create it. This can be done on the same server or elsewhere. There are advantages to both, and both should be done. Local backup can be used to gain quick access to alternate revisions. Offsite copies tend to cost a little more, but can protect you from viruses and other attacks.

Business continuity refers to what to do when there is an impact to service. For example, with hosted phones, how do you continue to do business if the power goes out? It isn't a disaster because

nothing is damaged, but there is a service impact. The service can be redirected to mobile phones, but a protocol must be in place.

Disaster Recovery is a plan more than a product. It refers to the replication of services. An example is having servers in multiple places. If one server fails, will another pick up? Is it immediate or must it be triggered? In some cases, systems can be inaccessible, but aren't down and manual intervention may be required or preferred. These are questions your provider can help answer.

In short, ask about each of these and understand the differences about how they can impact your business. In reality, you may not be able to afford 100 percent uptime, but understanding the areas of risk is crucial and a company's responsibility.

COOR: There are many technical options for data backup and disaster recovery. As with all IT, it starts with understanding the business needs, risks, compliance requirements, etc. and aligning the solutions to those requirements.

This should also be an ongoing dialog between IT and the business to educate on the various options, limitations and cost vs. capability trade-offs. For example, the business may need the critical accounting systems backed up offsite and available for disaster recovery with seven years of history, where the CRM system may be fine with just daily backups for 30 days.

SCOTT: Ask yourself, "If our data were lost or otherwise compromised, how long would it take to get operations back up and running from a back up?" Simply grabbing and dumping all of your data onto some back up media only thinks about the "disaster" but not the "recovery" aspect.

If an important document were corrupted, can you retrieve a copy of just that one file from your backups, or would you need to reinstate an entire machine to that last good state? How many other files might be lost for the sake of this one file? If you do need to bring up an entire machine or all of your sales records, how many hours are you waiting until it's back where it needs to be?

MEREYDE: Ideally, data should be backed up locally and remotely via a cloud backup data provider. It is very important to consider speed and security.

Some online backup data options can really slow down your system. Some software gives you options and settings that can be modified to schedule backups when you are not working, etc…

In the event of disaster recovery, you should chose a company that can overnight you your backup in a physical drive such as a USB. Downloading all your lost data online can take a long time. You should also consider a company that lets you access specific backed up files in the event you lost them and need access urgently.

What preventative measures can companies take to avoid cyber attacks, viruses and other threats?

COOR: The first and most important measure is education. All the technology processes, procedures and solutions can be in place, but without continuing user education, it is limited at best.

Most security issues are due to human error by clicking on that one seemingly harmless email or link that exposes the entire company. Security training should be part of any new hire process and ongoing to keep users up to date. Simple education for users on what sites to avoid, what common virus attachments look like and how attackers work can go a long way to mitigate risk.

From a technology perspective, each end user device should have most up to date, standardized virus protection software. Each office location should have up to date firewall protection. Any services provided by third-parties or hosted outside the company should receive confirmation from those providers what security measures are in place within their hosted environment. Your IT provider should offer training on what to look for and be a proactive set of eyes to keep your users safe.

MEREYDE: Ensure that you and your employees avoid questionable web sites or unknown web sites. Invest in a good firewall and antivirus software. Again, security and performance are key issues. Some antivirus programs are secure, but slow down your computer so much that you lose productivity. You have to look for the right balance.

You should pick hard passwords. Use a site like howsecureismypassword.net to determine how secure your passwords are.

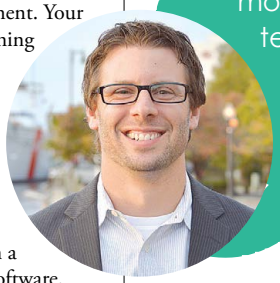
If you use Wordpress, consider plugins like the Wordfence paid version that gives you "two factor authentication." It sends you a text message on your cell phone to login.

Finally, use a secure VPN service if you are going to use any public WiFi.

SCOTT: Good security is mostly good policy. Even a bad thief knows to check under the welcome mat for a spare key. That being said, most of your attacks come in through the front door, so to speak.

Your office security can be locked down completely, but if an employee uses the same password for his Facebook as he does to login to your billing software, your business doesn't even need to be breached for them to get credentials to your finances. A good password policy and auditing plan can help this, and it's best to have someone in charge of this. Keep it scheduled and enforce changing passwords, or implement two-step authentication.

If your business runs under a Bring your own Device (BYOD) structure, creating a strategy can be a real pain, but even a simple plan can help avoid huge threats. Catalog each device that an employee may bring that connects to your network. That means phones, tablets, laptops, and even USB sticks. This will give you a real idea of what threats you might be bringing into your network from the outside and will let you know what type of BYOD policies you truly need.



"Companies need to determine their business model, and then ensure their technology supports their business model, rather than drives their business model."

SHAUN OLSEN
CloudWyze

OLSEN: Security is huge and, in all reality, measures can be taken (and should) but it is impossible to avoid everything. The best way to avoid issues is to be smart in your approach and separate, as much as possible, personal data from business data.

Virtual infrastructure, like virtual servers and hosted desktops, is great for this because IT can focus on protecting the core business technology and mildly manage personal technology. The basic precautions which can be taken are backups, centrally managed antivirus (meaning updates are forced, issues reported back to IT and users cannot disable or alter the application), patch and security updates are managed and automatically updated, DNS filtering and, ultimately web filtering/blocking is in place.

Remember, there is no 100 percent sure way to protect everything. Viruses, just like human viruses, can only have an antidote created if someone gets it first. Recently there have been viruses that attack backup programs and then locking the data. This is known as ransomware, and it is a big deal right now. Onsite backup is not enough.

How can companies combat ransomware? This is where victims have their data held hostage and must make an online payment to get it back.

SCOTT: Ransomware is scary because the sudden realization is that someone has been slowly hiding away your data for probably months, and you won't find out until they've managed to lock it up. Unless you have your data somewhere else or on another machine you can work on, then you're stuck paying a hacker what they ask or having to abandon that data together.

That being said, the best way to think about it is this: How would you manage if your phone or laptop were stolen? That is usually the answer to ransomware. The hacker is relying on you not having a

plan B.

Backup your data and scan your machines for malware often. Keep in mind, you want to make sure your backups are also clean from the ransomware infection. It does no good to find out that your backed up data is already encrypted and unusable, or that recovering your data also recovers the ransomware and starts the process all over again.

GARNER: The number one thing you can do to protect yourself from ransomware is to have a good backup. Notice I said good? Only having 1 copy of your data is a recipe for disaster. Sometimes it may be a day or two before you realize that a portion of your data is encrypted with ransomware. Therefore, having several days or even weeks of available versions of your data is absolutely necessary.

File sharing services like Dropbox should not be used as your primary backup solution. Likewise, you should not rely on the Windows Shadow Copy service. Many ransomware attacks can disable this service.

Beyond having a quality backup, there are a few additional things we recommend. First, ensure Windows and third party updates and patches are installed across your network. Secondly, you have to have a high quality anti-virus program that is updated daily. Finally, we recommend using a quality spam filtering service.

OLSEN: The best ways are to get multiple sets of data offsite into a secure facility and ensuring quick and easy access… and test it. Secondly, test it.

To be preventative, ensure people in your organization have limited access to install applications and make sure they do not open something that they don't know who sent it. Zip files, pictures and links can all be suspect.

A server-based group policy is a great way to limit user's ability to install applications, but smaller companies (and larger ones) have moved away from onsite servers. That said, a local group policy on a computer-by-computer basis can be implemented, but it is cumbersome to manage. In these cases, I would look to hosted infrastructure or "servers/desktops in the cloud."

MEREYDE: Do not download anything you do not know. Do not click on random links. Should you be the victim of ransomware, do not yield to their demands. Contact your IT professional to clean up your system.

COOR: Ransom viruses are just one of many threats that can be mitigated by following the same procedures for overall security. The critical aspect for any company is to have defined processes on how to handle a potential attack that includes a response team with defined escalation procedures and steps. Timing is critical with any ransom virus, so predefined procedures with rapid response and decision making with business owners is critical.

What are the most productive ways that companies are using cloud services?

GARNER: Generally speaking, cloud services should be the number one choice for email, data backup, anti-virus and spam filtering. There are many others, such as voice services (hosted PBX). These four tools are essentially requirements in today's business environment.

"Instead of paying $1,500 for a software suite, payment models like the ones you see for Office 365 and Adobe Creative Cloud allow you to pay an almost negligible monthly fee for it."

DEVON SCOTT
BlueFission

The main reason to migrate these services to the cloud is cost. Let's take email as an example. Implementing a local Exchange server is not only expensive and complicated, it requires a lot of upkeep. Additionally, most cloud services simplify the management and maintenance of the service compared to locally installed versions.

COOR: Most simply put, cloud services allow companies to get out of the IT business. Cloud services allow companies to invest in their business rather than in traditional onsite hardware, software and support services. The savings in these areas alone are significant.

In addition, cloud providers have much larger investments in technology infrastructure, security and redundancy, which can result in direct benefits to the company in higher service levels, guaranteed uptime, 24/7 support, etc., which a single company cannot afford.

MEREYDE: Cloud services can greatly enhance collaboration. They can also give employees more chances to telecommute therefore boosting employee morale and happiness.

OLSEN: Office 365 is big, but unless your business only uses Microsoft applications, it will have to combine with something else. An example would be an accounting platform like Quickbooks. Unless you go with the cloud versions of those applications, you start to build a disparate system.

This creates a huge problem for those who aren't savvy. In these cases, virtual desktop infrastructure (VDI) can be very appealing. VDI is great because everything happens in one place and can be centrally managed, protected and backed up.

It is also great for scale because users can be created quickly as well as blocked from access quickly since their desktop is streamed to them rather than local. The downsides are cost and internet dependency.

SCOTT: Cloud based services are the ultimate off-site backup. Employees can look up or update data from their home or on the road. This means an enormous increase in business agility. It also means that, when upgrading computer hardware, the time to install and configure services is greatly reduced. This goes especially for cloud based software and cloud based storage solutions that sync your data and activity across machines automatically.

Another great aspect of many cloud based services is the pay-for-use model, which allows you pay for how much you use certain services or how many users you give access to it. This means that you hold a huge amount of financial control and can trim fat methodically to really manage your costs.

Should companies have security concerns about cloud computing?

COOR: Companies should always be aware and concerned about security regardless of how and where the computing is done. However, cloud companies invest far more in security than an individual company can afford, so their security tends to be much more comprehensive.

MEREYDE: Companies should ask questions about encryption policies and where the cloud provider keeps their servers. How are they protected from intrusions, natural disasters and other threats?

OLSEN: Companies that use the internet should be concerned about security. Cloud is no different. Ensure your data can be exported, ensure your employees are trusted, change your passwords regularly (at least every 30 days) and have a policy in place when an employee leaves. Most security breaches in an organization are triggered by an employee.

SCOTT: The cloud is generally more secure than your own datacenter. On one hand, you have the security of "owning" your systems when you have in-house technology, at least in a geographic sense. However that means all responsibility for those systems falls on you. A reliable third-party cloud company dedicated to the storage, management and encryption of your systems and data will manage the infrastructure while you manage your business.

GARNER: Security should always be a concern these days. I believe, however, most reputable cloud platforms are safe. The reality is that in many cases, cloud-based solutions are safer than most small business network environments. Let's take cloud-based data backups as an example.

The offsite backup solution we provide encrypts your data before it sends it up to the cloud. If we were backing up your data to an external hard drive connected to your server, we typically wouldn't encrypt it. If the drive were

lost or stolen, your data would be in the open. That wouldn't happen with the cloud-based backups.

Other cloud services, such as remote servers, would also typically be more secure than most local networks. They would be physically more secure and the backend engineering that went into getting them online would be more robust than a typical local install. Other technologies, such as two-factor authentication, can be incorporated to improve security.

Which online collaboration tools are most effective for businesses?

MEREYDE: I personally like Google Apps for Work. They feel very familiar to a lot of users so the learning curve is usually not an issue. In addition, they can be accessed anywhere you have an internet connection on almost any type of device.

OLSEN: This is tough if you consider it from an application perspective, but I would say the most valuable concept is centralization. Having one user that connects via Dropbox and another that VPN's in and another that doesn't know how to connect remotely (or that it is even an option) is problematic. That said, email and chat are still number one. The challenge is capturing the data.

Lync or Skype, if integrated properly, is great since there is a trail.

SCOTT: Regarding communication, HipChat has gained a lot of support. You can bring people into project conversations and control who gets alerted to what you need. Being an Atlassian product, it naturally plugs into several of their other tech tools if you ever find yourself growing in those directions.

Slack is a great collaboration tool that acts as an internal chat system for your teams. While it isn't my favorite interface, it is very effective at what it does. In projects with several points of contact and many communications mediums (email, Dropbox, chat, text message, etc) it can be next to impossible to keep track of every asset, contract, and call to action. One search in Slack can look through all of these different sources to bring all of those conversations into one place.

I could recommend any number of project and task management tools, but none of them are one size fits all. Trello hits the mark by being broad enough to visualize what most businesses would have going on using Kanban boards and tagging features that have a fairly smooth learning curve. Google Drive is also still a very effective tool for collaboration. It provide cross platform multi-user editing, fairly simple but powerful sharing, security mechanisms, and powerful document and spreadsheet interfaces.

COOR: It's really business use specific. As a part of the business plan, leaders should decide how they see their users communicating. Is there a call center type environment? Will there be heavy inbound verse outbound calls? Do businesses need to monitor calls, record for training or development? Is there a need for instant messaging or short text type conversations that can be used internally and externally? Is there a need for high definition video calls and desktop sharing?

Combining all these methods is called unified communications and the trend most companies are moving to.

What should companies think about when selecting an Internet plan?

OLSEN: Buy what you need. More does not always mean better.

Internet is vital to just about every business today, but as businesses migrate to datacenters and utilize cloud services more, reliability and quality has become crucial. For years, larger businesses have chosen the option of synchronous Dedicated Internet Access (DIA), and that trend is trickling down to smaller businesses.

DIA should be standard for any business which has a critical component offsite, phone ad email included. If you have a choice, go with a guarantee and work with your provider to determine how "much" you need as it is best to have what you need and have it be reliable, than randomly have more than you need and no commitment to get you back up and running when it goes down. Leave best effort at home.

Additionally, don't put all your eggs in one basket. "Internet diversity" is big right now. If you are down, kicking and screaming to your provider may not get you back up and running if there is a fiber cut or DNS issue? Get an alternate provider in place and protect yourself. Paying $1,500 annually is a small price to pay for the security of a backup provider.

SCOTT: You want to know the strongest infrastructure in your area. If you are near your service provider, DSL or fiber optic can be preferable. If your cable provider's isn't saturated with competing users, you might win there. If your location is remote from the main town, you might want or be stuck with satellite. Also ask any existing customers in your area how well the service has been for them.

Also, estimate how much data you are actually sending and receiving and talk to your IT team about the bundles the provider is offering. Some providers offer phone lines, antivirus and spyware monitoring, and several other features.

"While allowing folks to remote into your network may seem complicated, in many cases, it is not. You probably have most of the technology already in place."

ROBBIE GARNER
Atlantic Computer Services

COOR: Companies need to plan monthly, for a primary and a secondary internet connection, from a different carrier. Even if the secondary is of lesser speed. By having two options, if something happens to the primary, although the speed may be slower, users can still access the hosted environment and work. If businesses have no internet, in most cases, production has ceased.

Companies need to plan their internet around their growth plans. It's crippling to try and do too much on too little bandwidth. Many businesses are migrating to internet (VOIP) phone systems, but don't have enough bandwidth to handle their data consumption along with phones. This gets back to the initial question of including the IT department/provider as early as possible in your business planning to ensure adequate Internet service is in place BEFORE deploying a new solution.

MEREYDE: What are the contract terms? Can I easily upgrade or downgrade my plan? What is the cost of renting versus buying equipment? What are download and upload speeds? How reliable is the connection?

How does the subscription model for software like Office 365 change the way companies buy and use software?

MEREYDE: The subscription model for software like Office 365 is cash flow friendly. In addition, companies do not have to worry about investing a lot in software that may quickly become obsolete.

OLSEN: It is the standard. Changes happen way too fast to buy software and small businesses need to be more nimble than ever before to stay competitive. Office 365 is taking over at least from a licensing standpoint, but it is rare you can use it for everything.

Unless you are buying traditional servers, it makes sense to subscribe and this goes for more than Microsoft. Adobe, Intuit, Sage and the like have all become service businesses. With that said, you may need to recalibrate your P&L to accommodate. Like it not, we're in a digital subscription age… music, car washes, gaming and, yes, software.

SCOTT: Instead of paying $1,500 for a software suite, subscription-based payment models like the ones you see for Office 365 and Adobe Creative Cloud allow you to pay an almost negligible monthly fee for it. This means that the investment for implementing, configuring, and learning the software is much lower, and it looks really good for

a company's cash flow. It's like getting a debt-free loan towards an expensive piece of software.

GARNER: It's a pretty safe bet that over the next couple of years, the only way you'll be able to buy business software will be based on the subscription model. Adobe and Microsoft are two of the most popular business applications that have adopted this model. In the past, we have purchased a copy of Microsoft Office and have assumed that the current version would last us 3 or 4 years. Those days are coming to an end. As for Microsoft, we're being pushed to their Office365 platform. You pay per user per month (or per year, if you wish).

Transitioning from buy it once and it will last a few years to per user subscriptions is a big pill to swallow for most people. There is, however, a bit of a silver lining once you understand what's included in the O365 packages. The basic package includes hosted Microsoft Exchange email, Skype for Business (Lync), online cloud storage, and web versions of the most popular office products. From the basic or Essential package, other plans add features such as local copies of office, SharePoint, etc. You could even roll voice services into your O365 platform. Prices start at $5 per user per month.

COOR: This approach allows for a simple buying experience versus a customized approach. The cost factor with this service is appealing for many businesses. However, there is a trade-off in service and support with many of these inexpensive subscriptions. The company should understand the services and support they will receive and confirm it will meet their business requirements. Many times the cheap option is not what is best for the business.

What is the most efficient and safest way to give employees remote access to company information?

SCOTT: Whether you have travel concerns, telecommuting, or contractors, remote access is an important thing to consider ahead of time. I avoid Remote Desktop Protocol (RDP) like the kind used by Windows Remote Desktop. The reason is not because of RDP itself, although there have been historic vulnerabilities with it.

The most important concern is securing your endpoints, which would be each device that connects to your business network remotely. Depending on how your employees really need to access data and how often, a simple browser based SSL VPN pass-through can connect your organization's members to the network with some simple rules. If you have more complicated needs, however, such as fully remote employees as well as some contractors who only need limited data, a combination of IPsec and SSL VPN access would give more control.

GARNER: While allowing folks to remote into your network may seem complicated, in many cases, it is not. You probably have most of the technology already in place. There are multiple ways to grant access into your network. The best solution for you will depend on what your users will be doing.

Most everyone is fairly familiar with a virtual private network (VPN). This simple approach to allowing access creates a secure tunnel for traffic between your office and the remote user. It can allow the remote user to access a corporate email system or to gain access to file storage. A downside of a VPN connection is that it can be very slow if working with larger files. It can become nearly unusable in some cases.

A more robust solution is to implement a terminal server at your office to allow remote users to log into. This solution is typically used when there is a business application to access.

COOR: Each user and department can have customized access based on needs. The first step is to define the level and type of access each group in the company needs. If group A only needs access to a particular piece of a software, which is different than group B and C, those requirements will be used when implementing remote access to ensure proper segregation and entitlement.

This procedure should be standardized as an onboarding process during the new hire process. The same should be defined when an employee leaves the company. Your IT provider should be able to assist in defining and implementing these procedures.

MEREYDE: Employees should have access to company information via a secure VPN. Employees should be given access to specific information on an as-needed basis. Using cloud services can also be a good option. Ensure that your connection is encrypted.

OLSEN: Efficiency, security and ease of use… VDI. Let's all agree that operating a desktop on a local network with a local server is quick, easy and manageable. VDI integrates that concept but gives the user a simple dashboard to connect into that environment.

It can be built on premise, but most are being built in datacenters. If done properly, it becomes the best of all worlds — great for the employer because he can control security, access, versions, scale, flexibility and costs. It is great for the employee because they can access their exact desktop from anywhere, any device and transferring data between colleagues is simple.

What factors should businesses consider before using Apple Pay, Samsung Pay, Square and other mobile payment systems?

MEREYDE: Train your staff. Offer choices. Do not abandon older payment options. Older customers may still prefer more traditional options such as checks or credit/debit cards.

OLSEN: A small fraction of you will be hacked and taken advantage of when compared the all the people using it. Be prepared, be careful and look into insurance to protect you against these breaches.

SCOTT: Most of these services have comparable features and fees, though some have slight advantages over the others. How do your customers pay you? If they pay via debit or through an app related to the payment service, they may or may not see the same fees as other customers. Also, what devices will your customers have? You don't want to alienate your customers because a mobile payment system isn't supported by their smart phone of choice.

Luckily there are services to mitigate this, such as Braintree, which processes most mobile payment systems including Bitcoin. If your customer is adventurous enough to experiment with the mobile payment system you are looking at, you can look forward to the improved security attached to each of these systems, including real time fraud protection, remote device deactivation, PIN requirements, and biome.

What is the most important technology issue that businesses should be focused on for 2016?

COOR: Given the increasing amount of security breaches, hacks and threats, the most important issue facing most companies will be information security. In the past, only the largest enterprises were targeted, but the landscape has changed and now the SMB sector has the same risk.

Having defined security policies, processes and procedures in place to secure company data is going to be a major focus for all companies; including how to respond in the event of a breach.

MEREYDE: Apple Pay and Samsung Pay.

SCOTT: Monitoring is a fairly big deal. Very often technology is put in place and never looked at again, or at least not looked at properly. Monitoring can mean the difference between being hacked and identifying a hack attempt, or almost more alluring, predicting a customer behavior that might signal your next flagship product or service.

Proper monitoring is also the first step for preparing for the Big Data world. Data can be very valuable and very marketable, but you will never know it is if you never collect it. Scanning, tracking, and monitoring your financial data, customer interactions, or web traffic is like choosing to make an investment in something you already have but have been throwing away.

OLSEN: Protecting their data and aligning their budgets to match the technology solution required to properly run their business.

Don't forget to call your helpdesk and say thank you every now and then!