INSIGHTful DISCUSSIONS

Sponsors' Content Distributed By Greater Wilmington Business Journal

TECHNOLOGY TRENDS FOR 2017

CHRISSY COOR
Director of Service and Business Development, Fluid IT Services

ROBBIE GARNER
President and CEO, Atlantic Computer Services

JOHN CORNELIUS
Owner, Wide Open Technologies, Inc.

SHAUN OLSEN
Founder and CEO, CloudWyze

DAVID USHER
President, CMIT Solutions of Wilmington

More than ever, technology is a critical component of a company's overall success. With ever-changing advancements and risks, it can be overwhelming for business owners to stay up-to-date on IT while also trying to manage their day-to-day operations. Five local experts share their knowledge regarding internet threats, data protection, best practices and trends for 2017.

What do you predict will be the top technology trend for businesses in 2017?

CHRISSY COOR: Remote accessibility for workers will continue to increase. Businesses will need to find ways to offer the work-life balance employees are looking for and, with this, will increase the need for higher security models to be put in place. Application sprawl will continue to increase as businesses consume their software applications directly from software vendors, creating more relationships to manage and more complicated support needs.

SHAUN OLSEN: While cloud adoption is all the rage globally, small- to medium-sized businesses (SMB) and small- to medium-sized enterprises (SME) in mid-markets are still trying to determine how to adopt and take advantage of these services.

In 2017, we'll continue to see small businesses working to migrate to hosted applications, such as Office 365 and Dropbox, but the big migrations will be the SMEs as they begin to transition to cloud platforms through providers like CloudWyze.

DAVID USHER: Artificial Intelligence (AI) and machine learning is quickly becoming a norm, not just a dream of science fiction writers. With intelligent applications and learning being built into the Internet of Things (IoT), we will see next year and for the foreseeable future more AI and machine learning as part of

INSIGHTful DISCUSSIONS

Sponsors' Content Distributed By Greater Wilmington Business Journal

"Today's focus to prevent security breaches should be on employee training."

ROBBIE GARNER
Atlantic Computer Services

"Most businesses are surprised to learn how many devices are connected and peting for limited resources."

DAVID USHER
CMIT Solutions of Wilmington

daily life.

In 2017, I see real exponential growth in IoT, and the very real challenge of how to manage and protect our businesses and ourselves as this massive increase in computing power comes online.

On a more optimistic note, I also see positive organizational disruption for businesses that foster employee creativity with regards to all of this new interconnectivity.

ROBBIE GARNER: At this point, migration to Office 365 should be on your radar. The first step may be just moving your email services over to the platform. If it's time to upgrade your company's Microsoft Office licensing, do it now. The immediate payback is your entire company will have the same version of Office. The bigger picture is O365 is a gateway to more advanced collaboration tools, as well as easy-access file storage.

JOHN CORNELIUS: There will be even greater emphasis on digital security in 2017. The combination of more companies and individuals moving data to cloud-based services and increased hacking attempts will make securing data more important than ever. We will see an increase in the adoption of multi-factor authentication, data encryption and password management tools. Online businesses will be under increased scrutiny when it comes to protecting customer data. Security breaches can drive customers to competitors and potentially lead to fines and other legal issues.

What is the biggest technology challenge facing local businesses?

USHER: How to manage connected devices across their network, both from a bandwidth consumption and security point of view. Most businesses are surprised to learn how many devices are connected and competing for limited resources. Typically, 25 to 90 percent of bandwidth consumption is non-business. On top of slowing down the network, this can also create significant security risks.

A commercial grade firewall manages the flow of information moving in and out of the business. It can prioritize important traffic, block bad actors and filter content to ultimately save money, improve security and increase office productivity.

CORNELIUS: As more businesses become dependent on technology, there will be more need for qualified technology staff and companies to provide those services. Trying to find and retain qualified people in a competitive environment is difficult. By definition, most qualified people already have jobs when there is a shortage of workers. Also, the excess demand will inevitably increase salaries and benefits you must offer to attract top talent.

GARNER: One issue we constantly deal with is affordable internet access. In Wilmington and surrounding areas, we do not have the same options as areas like Charlotte and Raleigh. Local access to fiber optic services can be expensive for a small company. Time Warner Cable has recently increased speed options for their business class services, which is a plus. As the cloud services trend grows, companies will feel more pressure to increase available internet bandwidth. That increased cost may prevent some companies from fully utilizing the cloud services available to them.

COOR: Keeping their data secure. As technology advances, so do the tactics used to breach security. Businesses need to stay proactive about their security. By staying ahead of expiring equipment, licensing and taking proactive training approaches, you can build a great defense around your data.

OLSEN: Confusion. With so many options, it can be confusing to determine what is needed to be successful. But approaching technology should not be much different than approaching any other business challenge. You should determine what is important for your business to flourish. If you are trying to grow quickly, scale may be more important than pinching pennies. In that case, you should work with a provider that can take as much off your plate as necessary for you to focus on growth and the challenges that come with it. If you are in cost-cutting mode then maybe you are willing to sacrifice some quality to funnel funds elsewhere. Either way, aligning your technology plan with your business plan is important.

How can companies ensure offsite employees in virtual workplaces are safely accessing sensitive information?

GARNER: Having remote users use a terminal server or virtual desktop infrastructure (VDI) would be a good first step. Both incorporate a virtual workspace into your environment, where users can access business applications and data, like documents and spreadsheets, but the actual data is being stored on the servers.

Beyond this, two-factor authentication is a common tool. In addition to username and password, the user has to enter a code that would be texted or enter a code from a token key. Many banks are doing this now. More common things like VPNs (virtual private networks) between the headquarters site and remote sites can also be implemented.

OLSEN: Deploying a service, such as VDI, is likely a perfect option, as it keeps the end-user desktop in the datacenter, meaning the data doesn't leave the facility. There are many ways to deploy this technology but there are certain variables common to all installations. A good provider will provide this information and ensure your solution meets all the required standards, as well as the operational ones.

CORNELIUS: Assume employees will access the internet from non-secure, public locations, such as coffee shops and airports. So, it is important that PCs and laptops are set up as securely as possible. This includes encrypting hard drives, using strong passwords and turning off unneeded services. It is also important that any services your employees will access remotely are secure. All services should only be accessible through secure connections. In the case of web-based services, this would mean a SSL (secure sockets layer) connection is required. For others - like remote desktop connections and anything requiring a connection into a company's data center - a VPN connection is highly recommended.

USHER: This is the age-old problem businesses have always had to address. Today, as employees work in a more decentralized manner, the risks have become more apparent. Think about that employee who accesses his or her email via phone and what types of information could be compromised if that phone is stolen. Is that phone password protected?

INSIGHTful DISCUSSIONS

Sponsors' Content Distributed By Greater Wilmington Business Journal

Employee training is a must. Part of the training must focus on the "why," so employees understand the risks are real. All mobile devices should be password- or passphrase-protected, and the hard drive should be encrypted. Acceptable use policies for mobile devices must be in place and should address texting and driving to reduce company liability. All remote communication should be through VPN.

COOR: Start by having a well-defined set of security policies and procedures that each employee must sign and adhere to, including an often-forgotten response plan in the event of a breach or attack. Ensure necessary security layers are included and deployed as a standard. Deploy more robust real-time monitoring and management tools and ensure the response plan has been tested and is ready to go. Human behavior will always be the number one security risk.

How can business owners determine if they are utilizing Office 365 and other cloud services optimally?

CORNELIUS: Having documents on a cloud service, rather than a local machine or server in an office, greatly reduces the possibility of data loss. Since most providers will keep a document's history, you are not only protected against accidental deletions, you can also look at previous versions of the same file.

The biggest reason to move to a cloud provider is the ability to collaborate on the same document simultaneously. This feature greatly reduces the amount of time needed for editing and contributing to a document.

OLSEN: You need to define the inefficiencies then evaluate which products solve which problems. Microsoft Office 365 is a very powerful tool but if the talent needed to deploy it requires someone to administer SharePoint then it may not be a feasible solution for you, despite the fact it may only cost $10 per user. Work with your solution provider to evaluate your requirements, as well as your abilities. The solution is out there.

GARNER: The O365 plan you have determines what you have access to. Beyond the most common Office products, there are tools that make collaboration easier. Chat, video conferencing, team workspaces and shared online file storage, when configured correctly, can all have a huge impact on information flow and efficiency.

The real potential comes from SharePoint, a platform for developing how your company handles data. Think of it as an internal website, where you can organize and manage data and set up workflows. If a document is changed, for example, SharePoint notify employees via email. While it's an extremely powerful tool, it takes effort to "program" the system to do what you want it to do.

COOR: Start by analyzing and understanding your specific business needs now and within the next year for each operational area. Take the time to define these requirements then identify the O365 and cloud services that best meet them. It is very easy to over- or under-invest in technology solutions, often with a direct negative implication to the business. Find a trusted IT partner that understands the changing technology landscape to ensure you have the right solutions at the right time. Ensure that your employees understand they play an integral role in the success of any technology solution and must be open to the learning and change that come with it.

"There is no silver bullet or one-size-fits-all for project management and collaboration."

CHRISSY COOR
Fluid IT Services

USHER: Purchasing software is only half of the solution. The value of software is a result of the training. Initial training must be designed to address some desired productivity gain to establish buy-in. After that, the training should be expanded and ongoing to keep existing employees engaged and train new employees.

If an owner already has a service, an experienced managed IT provider can work with the company to identify productivity opportunities and provide training. If the owner is considering purchasing O365, I recommend also purchasing a training-as-a-service option. It will be worth every penny.

What can a business do beyond file backups to ensure data is protected during a disaster?

OLSEN: Complete a disaster recovery plan (DRP) and a business continuity plan (BCP). Protecting data is different for all companies, as some businesses centralize data and some have it scattered among different services and applications. IT would prefer all data be centralized at some point then backed up for a defined retention period. What you should not do is rely on ignorance. Assuming something is taking place and not checking when you are the one impacted is no one's fault but your own. Create a plan to test your systems and don't overthink it.

GARNER: Companies should be thinking beyond basic data backup and about backing up whole servers instead. If you just back up data and your server fails, someone has to fix or replace the existing server, possibly reinstall software and then restore data. Depending on the severity of the crash and where the data is located, this could take several days.

If you had images of your whole server available, you could possibly be back up in minutes. Image backups are typically hardware-independent, meaning the image of your server could be spun up on a different machine, even a laptop. Once that system is in place, those images can be sent to offsite locations. Being able to quickly bring your servers back online in the event of a disaster is the direction you should be moving.

USHER: Most business owners know they need a DRP but most don't have a written plan. Developing a DRP or BCP is daunting because of the way we approach them. Typically we start with a disaster, like a hurricane, and become quickly overwhelmed by the scope of the plan. I recommend starting small by first identifying critical processes within the business and what could interrupt them. Find solutions for those then build upon your plan.

COOR: Ensure anti-virus protection is in place. While no anti-virus is 100 percent impenetrable, having this in place is a great first line of defense. Anti-virus protection can be installed on the end-user device (PC, laptop, tablet, etc.) but also on the servers, whether hosted in the cloud or on premise.

In the event of a true disaster, rapid access to critical applications and data is essential. It is not good enough to just back up your data because the data is only useful if you can recover it and it is usable, recent and accurate.

Businesses must be diligent and disciplined in regularly testing data recovery and use, which requires a written DRP involving many parties – employees, contractors, vendors, suppliers, etc. If any in the chain are left out, the entire recovery process is in jeopardy.

CORNELIUS: Make sure all backups are offsite, preferably in a different region. Having data available in another region allows for restoring service in the event of a widespread power outage or other event that might affect an entire region.

When choosing a location for backups, consider whether a natural disaster could cause an outage at both the primary and backup sites. For example, having your main datacenter on the North Carolina coast and the backup in Virginia may not be the most resilient design.

For files that change often, it is recommended that both backups and version control be implemented. This second level of protection not only guards against a file being lost, it also ensures a file that was inadvertently changed can be rolled back to a previous version.

What does the changing face of

Employee training is a must. Part of the training must focus on the "why," so employees understand the risks are real. All mobile devices should be password- or passphrase-protected, and the hard drive should be encrypted. Acceptable use policies for mobile devices must be in place and should address texting and driving to reduce company liability. All remote communication should be through VPN.

COOR: Start by having a well-defined set of security policies and procedures that each employee must sign and adhere to, including an often-forgotten response plan in the event of a breach or attack. Ensure necessary security layers are included and deployed as a standard. Deploy more robust real-time monitoring and management tools and ensure the response plan has been tested and is ready to go. Human behavior will always be the number one security risk.

How can business owners determine if they are utilizing Office 365 and other cloud services optimally?

CORNELIUS: Having documents on a cloud service, rather than a local machine or server in an office, greatly reduces the possibility of data loss. Since most providers will keep a document's history, you are not only protected against accidental deletions, you can also look at previous versions of the same file.

The biggest reason to move to a cloud provider is the ability to collaborate on the same document simultaneously. This feature greatly reduces the amount of time needed for editing and contributing to a document.

OLSEN: You need to define the inefficiencies then evaluate which products solve which problems. Microsoft Office 365 is a very powerful tool but if the talent needed to deploy it requires someone to administer SharePoint then it may not be a feasible solution for you, despite the fact it may only cost $10 per user. Work with your solution provider to evaluate your requirements, as well as your abilities. The solution is out there.

GARNER: The O365 plan you have determines what you have access to. Beyond the most common Office products, there are tools that make collaboration easier. Chat, video conferencing, team workspaces and shared online file storage, when configured correctly, can all have a huge impact on information flow and efficiency.

The real potential comes from SharePoint, a platform for developing how your company handles data. Think of it as an internal website, where you can organize and manage data and set up workflows. If a document is changed, for example, SharePoint notify employees via email. While it's an extremely powerful tool, it takes effort to "program" the system to do what you want it to do.

COOR: Start by analyzing and understanding your specific business needs now and within the next year for each operational area. Take the time to define these requirements then identify the O365 and cloud services that best meet them. It is very easy to over- or under-invest in technology solutions, often with a direct negative implication to the business. Find a trusted IT partner that understands the changing technology landscape to ensure you have the right solutions at the right time. Ensure that your employees understand they play an integral role in the success of any technology solution and must be open to the learning and change that come with it.

"There is no silver bullet or one-size-fits-all for project management and collaboration."

CHRISSY COOR
Fluid IT Services

USHER: Purchasing software is only half of the solution. The value of software is a result of the training. Initial training must be designed to address some desired productivity gain to establish buy-in. After that, the training should be expanded and ongoing to keep existing employees engaged and train new employees.

If an owner already has a service, an experienced managed IT provider can work with the company to identify productivity opportunities and provide training. If the owner is considering purchasing O365, I recommend also purchasing a training-as-a-service option. It will be worth every penny.

What can a business do beyond file backups to ensure data is protected during a disaster?

OLSEN: Complete a disaster recovery plan (DRP) and a business continuity plan (BCP). Protecting data is different for all companies, as some businesses centralize data and some have it scattered among different services and applications. IT would prefer all data be centralized at some point then backed up for a defined retention period. What you should not do is rely on ignorance. Assuming something is taking place and not checking when you are the one impacted is no one's fault but your own. Create a plan to test your systems and don't overthink it.

GARNER: Companies should be thinking beyond basic data backup and about backing up whole servers instead. If you just back up data and your server fails, someone has to fix or replace the existing server, possibly reinstall software and then restore data. Depending on the severity of the crash and where the data is located, this could take several days.

If you had images of your whole server available, you could possibly be back up in minutes. Image backups are typically hardware-independent, meaning the image of your server could be spun up on a different machine, even a laptop. Once that system is in place, those images can be sent to offsite locations. Being able to quickly bring your servers back online in the event of a disaster is the direction you should be moving.

USHER: Most business owners know they need a DRP but most don't have a written plan. Developing a DRP or BCP is daunting because of the way we approach them. Typically we start with a disaster, like a hurricane, and become quickly overwhelmed by the scope of the plan. I recommend starting small by first identifying critical processes within the business and what could interrupt them. Find solutions for those then build upon your plan.

COOR: Ensure anti-virus protection is in place. While no anti-virus is 100 percent impenetrable, having this in place is a great first line of defense. Anti-virus protection can be installed on the end-user device (PC, laptop, tablet, etc.) but also on the servers, whether hosted in the cloud or on premise.

In the event of a true disaster, rapid access to critical applications and data is essential. It is not good enough to just back up your data because the data is only useful if you can recover it and it is usable, recent and accurate.

Businesses must be diligent and disciplined in regularly testing data recovery and use, which requires a written DRP involving many parties – employees, contractors, vendors, suppliers, etc. If any in the chain are left out, the entire recovery process is in jeopardy.

CORNELIUS: Make sure all backups are offsite, preferably in a different region. Having data available in another region allows for restoring service in the event of a widespread power outage or other event that might affect an entire region.

When choosing a location for backups, consider whether a natural disaster could cause an outage at both the primary and backup sites. For example, having your main datacenter on the North Carolina coast and the backup in Virginia may not be the most resilient design.

For files that change often, it is recommended that both backups and version control be implemented. This second level of protection not only guards against a file being lost, it also ensures a file that was inadvertently changed can be rolled back to a previous version.

What does the changing face of

INSIGHTful DISCUSSIONS

Sponsors' Content Distributed By Greater Wilmington Business Journal

hacking currently look like, and what threats does it pose to businesses, large and small?

COOR: Even with the obvious increase in security breaches and hacks - and ever-increasing media coverage of them - business owners, especially small- to mid-sized, often ignore them, believing it won't happen to them or they don't have the time or money to deal with it. The reality for all businesses is being hit with a security incident is not a matter of if but when.

Because a majority of security incidents are due to human error, it all starts with training. Beyond that, standard security solutions - firewalls, secure wireless access, anti-virus and acceptable use policy - are the foundation of protection. A third-party annual security assessment from an IT company is also an excellent way to understand and remediate ongoing risks and issues. Security-as-a-Service is also a relatively new highly specialized offering that can handle and address security for specific aspects like compliance with HIPAA or PCI (Payment Card Industry).

USHER: What has happened over time is larger businesses have built better defenses and smaller businesses are becoming the easier target. SMBs not only provide a source of revenue; they also can be a gateway to a larger company's data. The Target hack is a perfect example. The hackers entered the system by first getting into a (now bankrupt) HVAC supplier in Pennsylvania and working their way up using the credentials of the HVAC company to eventually hack into Target.

We recommend cyber liability insurance because you are not only liable for your data and that of your employees; you are also liable for the data and access to your customers' and suppliers' systems.

CORNELIUS: One reason for an increase in attacks is the increasing number of devices – including webcams, networked home appliances, televisions and wearable technology - connected to the internet. Many of these can be hacked similarly to a PC, so users should take precautions. Default passwords should be changed where applicable and secure WiFi should always be used to connect devices. Compromised devices have the potential to launch DDoS (distributed denial of service) attacks. Secondly, if the compromised device lives inside a victim's network, it could grant attackers local access to other machines and devices inside that network.

OLSEN: We see that the biggest issues with the most impact to businesses are less related to technology and more to non-technology, specifically, social engineering, or taking advantage of human nature. Educate your team on phishing emails and be careful what you open. Good providers will make you aware of what can be done proactively and show you pathways to implement them, whether it is to install an appliance, subscribe to a service or send you blog posts or articles like these.

"The biggest reason to move to a cloud provider is the ability to collaborate on the same document simultaneously."

JOHN CORNELIUS
Wide Open Technologies, Inc.

GARNER: Today, hacking is big business. There are entire organizations in other countries that do nothing but try to steal money. The sad thing is that they are good at it! So, what is a company to do?

It should be a no-brainer to use a quality antivirus program on all company computers and update that program regularly, as well as conduct Windows and third-party updates. The network should have high-quality firewall and spam filters in place for email.

With all this, you're still vulnerable. The real target these days is unsuspecting employees. By clicking a link or unsuspectedly talking with a fake support agent, they simply let hackers in, bypassing all of the security layers you have in place. Today's focus to prevent security breaches should be on employee training.

How can business owners be proactive about security?

USHER: It's important for business owners to recognize that their data or who their business is connected to is valuable to someone. With this in mind, here are a few steps every owner can take. First, have a strong password policy. Conduct periodic training. Purchase a commercial-grade firewall to create a secure perimeter. Finally, update all hardware and software with the latest patches and manufacturers' updates. It should be noted though, that the greatest security risk is still the space between the chair and the keyboard.

COOR: Proactivity starts with awareness and training. Even with the best security solutions in place, it only takes one employee to click on "that link" to bring the entire business down. In addition to training, implementing security services that are constantly monitoring your business is one of the best ways to stay proactive and remediate issues before they happen. Additional policies and procedures - such as preventing any company data from being stored on an employee's computer and only in a secure cloud environment - can go a long way.

CORNELIUS: All systems, including servers, personal computers and other connected devices, should be up-to-date with the latest software patches. Most operating systems can now automatically apply security patches as they are released. Not applying patches in a timely fashion can leave you vulnerable to attacks.

Systems should also have protection software installed to guard against viruses and other potential threats. It is important that protection software is set to automatically update. Businesses can stay up to date on new security threats by subscribing to security bulletins for the operating systems they use.

GARNER: Assuming all basic security measures are in place and actively managed, it is imperative to provide IT training to employees. When an email comes in to an accounting clerk from the company president asking for a wire transfer, what will he or she do? Dismissing this as something that happens to other companies is naive. It happens every day.

Another situation we've seen is a window pops up on a user's computer that reports a virus or other problem and provides a support number to call. When the employee calls, they allow the fake support agent to remotely enter the PC.

Both of these examples have happened locally, and the companies had all basic security measures in place. If we don't train our employees on security, we are leaving ourselves vulnerable.

OLSEN: Know your risks based on your current system and do as much as you can afford. There are so many inexpensive services on the market, from antivirus and DNS (domain name system) filtering to mail and web filtering, which can provide a level of security close to that of a large enterprise. Additionally, small businesses can work with companies like CloudWyze to deploy more comprehensive services like Active Directory or Group Policy to limit users' ability to "break things" related to the business.

What do businesses that process credit card payments need to know about the new version of the federal Data Security Standards that went into effect in November?

CORNELIUS: Rather than just an annual assessment and report, companies must now constantly monitor their systems and IT practices for compliance.

Another important change is administrative accounts must use multi-factor

INSIGHTful DISCUSSIONS

Sponsors' Content Distributed By Greater Wilmington Business Journal

authentication to gain access to credit card information. Multi-factor authentication involves users providing two or more different types of information to the system: knowledge (something they know); possession (something they have, such as a card or token) and inherence (something they are, such as biometric characteristics).

An example of this would be an ATM card. To use your card at an ATM machine, you must have the card itself (possession) and your PIN (knowledge).

USHER: Many small businesses incorrectly feel that as long as they use a credit card processor that promises an encrypted connection and no local customer data storage, they are covered. The credit card processor does provide a significant layer but the small business is still required to complete a self-assessment questionnaire (SAQ) designed to ensure its practices are secure. There are multiple questionnaires, so a business must first determine which one is fitting.

And processes surrounding penetration testing have been strengthened and those tests are required with greater frequency.

COOR: The current version of the standards – DSS 3.1 – will expire six months after the release of DSS 3.2. Consequently, all updated SAQ forms and procedures should now be used. However, these new components will not become a requirement until Feb. 1, 2018, in order to provide companies sufficient time to implement the new standards.

It is recommended that companies/merchants commence an immediate review of their current authentication protocols and begin to upgrade those systems to comply with the new standards on an expeditious basis. It is also critical to build enough time into this process to allow for proper training of affected employees to avoid last-minute implementation difficulties and meet the Feb. 1, 2018 deadline.

OLSEN: Work with an expert to ensure you have the proper items to maintain compliance within your environment. If you don't understand something don't ignore it. Have it explained and ensure you define clearly what you need to do in order to be compliant, then do those things and document them. If it is hyper-critical to your business then value that expert appropriately when shopping around.

What questions should a business owner ask when shopping for an IT provider?

GARNER: For every IT issue\project, there are multiple ways to make it happen. This is where experience and expertise come into play. You want to be sure your potential provider has experience with cloud services. The best way to get this information is to ask them directly for references.

Most folks are nervous and uncertain about technology, so it is important to have a working relationship with your IT provider. Getting past flashy sales presentations and down to their real abilities is key. You want to do business with someone you can trust and who is looking out for your best interest.

OLSEN: Do you understand our business? Do you know what we want? Can you tell us what you think we need? Have I given you enough information? What am I not thinking about? Can you grow with us? Can you provide me with at least three references?

USHER: I am going respond with what an IT service partner should do for a business owner, and should do well: identify high-risk aspects that demand immediate attention; provide proactive 24/7 systems monitoring; implement services that fit the budget and needs; develop long-term action plans for hardware, software and support upgrades; and most importantly, listen.

An IT service partner should serve as a trusted advisor that understands your overall business goals, hears your concerns, asks questions about your technology needs and focuses on ways to improve your productivity and profitability.

COOR: First, the business should determine the scope of its needs and wants. Do you have no internal IT staff and therefore want comprehensive IT services and management from a single company? Do you want to augment your existing IT staff with specific services? Good IT management companies will offer a wide range of services to handle all IT needs.

At Fluid IT Services, we own and manage our own cloud hosting service, along with security, disaster recovery, helpdesk, procurement services and software licensing services, as well as being a Microsoft Cloud Solutions Provider for all Office 365 and Azure products and others. As a result, we can provide end-to-end IT services or specific services.

If you are unsure of your needs, the IT company should guide you through the process, helping identify your needs and providing options, ideally with a comprehensive IT roadmap.

"With so many options, it can be confusing to determine what is needed to be successful."

SHAUN OLSEN
CloudWyze

CORNELIUS: Be sure the company has handled projects similar to yours. Some companies will take projects with unfamiliar technologies and try to get up to speed. This can cause delays or mean poor-quality work. Also note that a lot of companies will try to persuade you to switch technologies to one they are more familiar with. While not always a bad idea, you should be sure that the change is being made for the right reasons. Always check references to see what other companies think. A good reference from a company similar to yours is invaluable.

What new online project-management and collaboration tools do you recommend for businesses?

COOR: There is no silver bullet or one-size-fits-all for project management and collaboration. Solutions should be tied directly to the business' requirements. That said, with the improvements to Office 365 and the addition of Skype for Business, there are some robust and affordable collaboration tools available. There are hundreds of project management tools ranging from free to thousands of dollars. Finding the right one should be done as a more formal solution selection process, where products are vetted, tested and, most importantly, the support and service levels from the solution provider are confirmed.

OLSEN: The real answer is it depends on what you are trying to accomplish. For some, the answer could be as simple as a spreadsheet or leveraging a current application like Salesforce, but for others, it may be something dedicated like Basecamp, Maven-Link or MS Project. Whatever the solution, setting the right expectation is key. Know what you want it to do, how you want to use it, who needs access to it and what you can do. Then, evaluate your options.

CORNELIUS: The biggest game changer for us has been Slack. We find it much more efficient than email. The inter-office email traffic has been dramatically reduced. Also, the integrations available make it easy to do things like launch conference calls and share files easily and without changing to another application.

USHER: The most important aspect of finding the best collaboration and project-management tools starts with looking inward at the culture of the business. It does not matter how great the tool is if employees and management don't embrace it.

A few products on my radar are Slack, HipChat, Asana and good old Microsoft. Microsoft Teams is a new collaboration tool available to Office 365 subscribers with a chat option that allows the users to share content within the chat.