IT Security Best Practices -- Executive Summary

Don't have time to read the entire "Vistage Best Practices: IT Security Best Practices" feature? Here are the key points in a brief executive summary.

Prevent Loss of Important or Sensitive Data with a Solid Backup Strategy

Every company needs a strong and reliable backup strategy — not just for the servers, but also for every computer and device the CEO and employees use. Fortunately, there are several backup options available. Which one to use depends on whether you're backing up the CEO's computer, an employee's workstation, or the company's server.

- **Image Backup**
  Think of an image backup like a picture of your computer, workstation, or server. It's an exact bit-by-bit copy — a clone, if you will. Unfortunately, Foster finds that many executives are not aware of image backup, and many IT departments are not using it either.Since an image backup is an exact duplicate of a hard drive or server, it can quickly restore a machine to its exact state at the time of the backup. This includes the operating system, the registry, the program files, the data files, and the computer or network settings. And all this happens in one fell swoop. It's like taking a snapshot of the computer or server.

- **Online Backups**
  Online backups are another option for personal computers, workstations, and servers. In this case, the backup takes place over the Internet and the data is stored on the service provider's server. Online backup services can typically backup whatever data you choose.

- **Cloud Storage (Cloud Backups)**
  What about cloud options like iCloud, OneDrive, DropBox, etc.? Are they secure, and a good backup option? They are probably relatively secure, but there's no way to be sure of servers over which you have no direct control. However, they are a valid option for both personal computers and work computers.

No matter what technology you choose for your backup strategy, whether you're backing up your personal computer, your workstations, or your server, test it often. Too many companies have failed when they mistakenly thought they had a backup but didn't, and then suffered a catastrophic loss of data. Perform formal testing at least once a quarter.

Important Points about Your Disaster Recovery Plan

All businesses need a Disaster Recovery Plan (DRP). A disaster can hit anyone at any time and can include such things as fire, theft, hurricane, long-term power outages, terrorist attacks, hacker attacks … the list is endless. Therefore, your plan needs to allow for the continuation of business in the event that one or more

servers, and potentially even an entire office or work location, becomes inoperative for any reason. The DRP includes provisions for rapid transfer to new servers and minimal, if any, downtime for users.

- **Spend Wisely**
  The key is to balance the cost of implementing the DRP with your needs. **Calculate the money you'll lose in the event that your company loses its network, and then multiply the costs by the percentage of likelihood of that disaster occurring.** This gives you a rough budget for your DRP. To tune that amount, you can calculate different costs and likelihoods for being down an hour, a day, and a week. This gives you not only a more accurate amount, but also a better idea of how quickly the network needs to be up and running again.When it comes to spending, do the most important preventive measures first, and then move on to the others as time and money permits.

- **Testing Is Crucial**
  You must test your DRP regularly. There's no point in creating a plan if you never know whether it actually works. If you're utilizing an outside company to help with the planning, tell the company that you need test it at least once a year — and if they can't accommodate that, you'll move to another company. Otherwise, you're not going to have faith that your plan will actually work.

- **The Biggest Overlooked Disaster**
  If your sole IT professional (or any key member of your IT team) was seriously hurt or ill, and couldn't come to work for any length of time, that's a disaster too — and you need to have plan for such a scenario. Remember, without your IT professionals, your company would suffer a loss that could be just as great as what would occur in the event of a natural disaster. Have a plan for everything. While the best-case scenario is that you'll never need to enact your plan, you definitely need to have one, just in case.

How to Effectively Work with Outsourced IT Professionals

Many companies outsource their IT needs and services. That is, they don't have any internal IT staff and bring in outsiders to handle that aspect of their company. Depending on your company and its size, outsourcing your IT may be a good decision. If you have a dedicated IT team on staff, chances are that they're extremely busy, so bringing in some outside help to assist your main IT staff could be a great idea.

- **The Cons**
  When your organization outsources IT support without the appropriate checks and balances, the tactic of "put out the technology fires but don't prevent the fires" can get out of control. Many companies really appreciate an IT vendor that's responsive and fixes problems. Unfortunately, they're also oblivious to the fact that the underlying problem is usually still there. Some outsourced companies are oblivious to the underlying problem, too; they feel their mission in life is to put out fires.Another problem is that too many organizations hire outsourced IT companies and pay them by the hour. But if you pay an hourly rate, what's the IT company incentivized to do? If you said, "take longer," then you are exactly right.Not only will they take longer, but outsourced IT companies can send inexperienced staff members to your location to respond to your requests. If those inexperienced people aren't familiar with what needs to be done, then they'll spend time educating themselves. Eventually, they'll likely solve the IT problem you wanted them to fix — but you just paid an hourly rate while they educated themselves.

- **The Pros**
  The biggest pro of using an outsourced IT provider is the level of expertise you can get. In the IT field, it used to be that one person could be an expert in everything technology related. But because technology has expanded so much over the years, that's no longer the case. Even so, many IT professionals still think it's their responsibility to do everything in the IT department. Often, this can cause problems. This is where an outsourced IT company can be most useful, because they usually have many people on staff, each with his or her own unique expertise.Additionally, outsourced IT professionals see many different businesses and often recognize problems early, before they have a chance to damage your organization. Even better, some IT outsource firms have alliances with vendors that can get you special pricing on hardware and software. Finally, should your own IT professionals move on or become ill, it's helpful to have a solid outsourced IT firm to fill any temporary gaps.

Grab the Reins of Technology Spending

Technology spending can quickly get out of control. Neither executives nor their in-house and/or outsourced IT professionals necessarily know where to cut costs. The following tips can help busy executives rein in costs.

1. Stop buying the most storage money can buy.
2. Think twice before paying for extended warranties.
3. Shop around.
4. Use the power of the hardware and applications that you have already invested in!
5. Do preventive maintenance
6. Use server virtualization to save money on servers.
7. Adopt workstation virtualization.
8. Consider buying refurbished equipment.
9. Don't pay outsourced IT by the hour.
10. Finally, stop killing alligators and drain the swamp.

Repel IT Attacks: Update and Patch Your Operating Systems and Applications

Regularly update your operating systems and applications to keep your computers and network safe. Attackers look for common weak spots on your network, and the two most common vulnerabilities are unpatched operating systems, such as Windows, and unpatched applications, such as Adobe Reader, Flash, and Java. That's why you want to keep your operating systems and applications patched and upgraded to the most recent version.

To simplify patch management for **operating systems**, use the following guidelines or best practices:

- Attackers constantly probe operating systems and applications to find vulnerabilities to breach your network, steal information, and control your machines among other activities. Vendors release patches on a regular basis and the patches need to be monitored daily.
- It's best to make sure all users have all "high priority" and "critical" patches and updates tested and applied within hours of their release. If you elect not to apply certain patches right away, then establish another control to mitigate or eliminate the risk this creates.
- Websites are a major source of attacks. Microsoft makes major security improvements with each release of Windows and each release of Windows Server. More recent versions of Microsoft's browser Internet Explorer (IE) are significantly better, including security, than any other prior Microsoft browser.

- For best results, deploy operating systems patches in a quality assurance (QA) test environment, as opposed to directly into the environment. During QA testing, carefully check all of your own applications that are not “main stream” applications and ensure that new operating system patches get tested first on non-production machines (or at the least, on a small portion of your production machines). Many organizations choose not to use a complete QA environment in favor of other testing methods, such as staged deployment and keeping snapshot images of their machines. Be sure your executives make an informed decision rather than leaving the decision to the IT team.
- Microsoft and other vendors generally stop focusing on patches to older versions of their operating systems. Eventually, support is dropped altogether. But upgrading to new operating system versions can sometimes create unstable systems and unexpected results, especially in relation to the other systems in your environment. So, even though you may not move immediately to new operating systems, strongly consider upgrading to the latest version within less than six months after release. Sooner is better from the standpoint of security, unless the new version has unexpected security flaws. It’s important to emphasize: Upgrades to the latest version *should not be confused with updates or patches*. Updates and patches need to be installed much sooner.

Prevent Your Remote Workers and Road Warriors from Devastating Your Business

These days, it’s common for companies to have remote workers and/or employees who travel extensively. Having people work remotely has many benefits, and having employees who travel to client locations does wonders for relationship building. However, there are also some definite security concerns when you allow people to remotely connect to your network.

The following suggestions will help keep remote workers from hurting your security.

- Some technologies can actually examine the remote machines before allowing a user to connect. If the remote machine does not meet minimum standards for security, the connection can be refused.
- Other technologies can publish programs to the remote computer in such a way that the remote computer’s interface is in a safety zone that is protected against most kinds of attacks.
- It’s too much work for an IT professional to go visit every remote computer on a weekly basis to check the security, so there are centrally managed solutions as well that automate this task. Your qualified IT professionals can help you identify the best solutions for your organization that allow you to protect the remote computers.

A common way to keep remote workers (and your network) safe are virtual private networks (VPNs), which enable remote computers to connect through the Internet as if they had an ethernet network cable stretched all the way from the remote computers to your company’s main office. This connection is helpful in connecting remote satellite offices as well as employees out in the field to the company’s network.

This simple VPN will help prevent one of your employees from coming back to the office and bringing viruses and other malicious items into the company’s network, because IT has a chance to regularly update, monitor, and service the machine. And best of all, the cost is very inexpensive, typically based on the number of connected users.

Know the Benefits and Dangers of Cloud Computing

By now most people have heard of the cloud. But there’s a big difference between storing information in the cloud, using a program or application that runs in the cloud, and moving completely to workstation virtualization in the cloud. There’s a good chance that your organization already uses a hybrid — i.e., mixing cloud services with your existing technology — and that’s fine. You may move more to the cloud, or not. The most important part of using the cloud properly is to increase returns, reduce costs, and improve both your users’ and

customers' experiences.

Whether to move some or all your services and applications to the cloud is a strategic decision. The good news is that, *if handled correctly*, the cloud can be very helpful for any size company.

Top 5 Questions to Ask Your IT Professional to Keep Your Company Safe

Because today's technology can be so complex, busy executives who want to know how to best utilize their technology resources often don't know what questions to ask their IT professionals. Use the following list of security-related questions to ask your IT staff today. Know the right questions to ask means you can rest assured that your company is adequately using existing technology resources to keep your company safe.

- **Question #1: "What security level is configured for the Internet and trusted websites?"**
  Modern browsers strive to make security settings easy and understandable by offering a few settings from which to choose. Browsers include IE (Internet Explorer), Firefox, Safari, Google Chrome, and others. These are examples of the protection levels: high security, medium-high security, medium security and pathetic security (but users will probably never complain). A really nice feature is that you can choose "high security" by default and then make exceptions for specific sites that you trust.Ask your IT professional to adjust, and at least discuss with you, the current settings on your organization's browsers. The default security settings for untrusted sites are probably set too low.

- **Question #2: "Are any of our users configured to be a local administrator on their computer?"**
  Attackers can cause a great deal more damage if your IT professional is so busy that they do not modify settings that are misconfigured in a "standard installation" of Windows. That's why you need to know whether any users are configured to be a local administrator on their computer.The proper answer is "No. None of the users have any administrative rights on their computers." If they answer in any other way, direct them to "fix it."

- **Question #3: "Do you have to reduce security for all of our programs to work properly?"**
  This problem stems from the fact that you've likely tasked IT with keeping your systems up and running, and that includes configuring applications and systems the way manufacturers dictate. IT professionals follow directions and often do what the manufacturers tell them to do.Your directive to your IT professional needs to be: "Find out what permissions and rights that software needs, grant those rights, and make the users standard users, not administrators." Your IT professional is very qualified already and can do this.

- **Question #4: "Do you trust the bank's software vendor?"**
  Counterintuitively, the bank often tells your IT professionals to disable important security protection. This happens when your bank gives you a program or website in order for your users to make online deposits, pay bills, calculate payroll, or do anything else related to banking.Often, banks tell your IT department to disable protections because their support staff (or more often, the company that provides services to the bank) want your banking services to operate without technical difficulties. If you experience technical difficulties, that reflects badly on the bank. You might change banks as a result, and banks understandably don't want you going to a competitor.So what do you do when the bank asks you to lower your defenses? You tell your IT person to keep security in place and to open up the bare minimum that the banking functions need in order to operate properly.

- **Question #5: "What's more important: security or productivity?"**
  You do need to keep productivity ahead of security. The caveat is that security needs to be *almost* as important as productivity.Password restrictions are a change that most users will notice. However, users will never notice many, in fact the majority, of security settings.The real issue: It is your role as the executive to make sure your IT team is implementing the protections that you wouldn't notice anyway.

Mike Foster is the founder and CEO of Foster Institute.

Expert Practices -- Your Data Backup Strategy

Prevent loss of important or sensitive data by creating a solid backup strategy. Here's an overview of how to get started.

Every company needs a strong and reliable backup strategy — not just for the servers, but also for every computer and device used by the CEO and employees. No one wants to experience data loss. For an organization, a loss of data can be disastrous. That's why Vistage speaker **Mike Foster** urges all companies to regularly re-evaluate their backup strategy and test their restore process to ensure it suits their current needs and adequately protects them.

Backup Options

Foster explains that there are several backup options available. Which one to use depends on whether you're backing up the CEO's computer, an employee's workstation, or the company's servers. Regardless of what you're backing up, follow the best practice of making a full backup at least once every 24 hours.

Foster offers the following overview and suggestions for each backup method.

1. Image Backup
Think of an image backup like a picture of your computer, workstation, or server. It is an exact bit-by-bit copy — a clone, if you will. Unfortunately, Foster finds that many executives are not aware of image backup. He believes that if executives were aware of this option, more IT departments would probably use it.

Since an image backup is an exact duplicate of a hard drive or server, it can quickly restore a machine to its exact state at the time of the backup. This includes the operating system, the registry, the program files, the data files, and the computer or network settings. And all this happens in one fell swoop. It's like taking a snapshot of the computer or server. Here's how image backup can help your backup process:

- **Personal devices:** Foster says that he performs an image backup of his computer every night, alternating between two different backup drives. And he urges CEOs to do the same for their own personal computers. Why? Because if your computer should ever crash (and you have to admit that would be a huge headache), you can restore it very quickly, even if you lose one of the drives.The time it takes to restore from an image backup depends on how much data is stored on the computer. Frequently, a restore can be finished in less than half an hour. That is one of the reasons image backup is so helpful: A 30-minute restore is much faster than having to wait for your IT professional to reload your operating system, reinstall your applications, and restore from a normal data tape backup.Two good image backup solutions for single computers that Foster recommends are Symantec Ghost from www.Symantec.com or True Image from www.Acronis.com.His favorite right now is ShadowProtect from www.StorageCraft.com. Of all these choices, Ghost is probably the easiest for a novice user.

  "If you download any of these from the Internet, pay the small fee to have them ship you the CD," he advises. "You definitely need the CD in case it is required during the restore process. When your computer crashes and you need to get it going again quickly, you don't want to find out then that you will need the CD. Sometimes for the restore process to start, you have to insert the product CD and boot the computer from that."

  With that said, make sure your computer actually will boot from the CD. Test it. Don't find out the hard way that it doesn't work. With many computers, you have to hold down a key during boot-up in order to tell the machine to boot from the CD. Sometimes it is as easy as holding down the C key. Here's a suggestion Foster recommends you do today: "Google the phrase: How to boot from CD computer-model. Replace the words 'computer-model' with the model of your computer."

  For backing up your smartphone and tablet device (like an iPad), Foster suggests regular synchronization with your computer or other system. Be sure the synchronization process includes backing up all the information on your phone or device. If you're not sure, ask your IT professional for help. Don't make the assumption that the synchronization process also includes your photographs; make sure. Don't lose photographs of your most memorable moments just because your synchronization doesn't backup your photos too.

- **Workstations:** An image backup works the same way on your employees' workstations as it does on the CEO's personal computer. While this in itself offers great advantages, your company will see the power of workstation image backups when your organization buys new computers or has to do updates to existing ones."Chances are your IT professional already uses image backup in some capacity," says Foster. "For example, with image backup, if you purchase six new computers, your IT team doesn't have to take the time to configure all six computers individually. In one sixth the time, they can configure just one computer, make an image backup, and use tools they know about to modify the image so it can be deployed on the other five computers. That way all six new computers are all the same."Having image backups of workstations can make workstation repairs very easy to perform. The computer can be quickly "reset" to the way it was when it was new, or the last time it was imaged. It's best if these images are kept up to date with the latest patches and are hardened effectively. Eliminate all unnecessary applications and services.

  Consider making image backups of your more important workstations so repairs can happen quickly in an emergency. Be sure to keep the images secure so unauthorized people can't modify them. Keep in mind the drive space requirements. Alternatively, you may use a tool such as Microsoft's WDS (Windows Deployment Services) to deploy new images to multiple computers. Microsoft's System Center tools also offer rapid deployment of operating systems and applications to your workstations to aid in support.

  For backing up tablet devices and smartphones, your IT department may elect to use one of the enterprise tools available that allows management of each device. Other benefits of those tools, in addition to the backup functionality, include support for automatic tracking, remote wipe of all data, and being able to secure the tablets and smartphones. Examples include Dell SonicWALL Secure Remote Access Appliances, Lumension Mobile Device Management and EdgeWave, among many other options. Use the one your IT professional likes the best.

- **Servers:** Image backups of servers are also vital. When a server crashes, rebuilding it can take a lot of time depending on the server configuration. Image backups of servers allow quick server restores when you need them the most. Just like it works with personal computers and workstations, you're getting a complete copy of the server. Two tools Foster suggests for server image backups are Symantec LiveState Recovery from www.Symantec.com and the server image backup offered by www.UltraBac.com.Additionally, companies that have adopted server virtualization using products by companies such as VMWare and Citrix don't necessarily need any add-on product to perform image backup. With server virtualization, your IT professional uses a software application to divide one physical server into multiple isolated virtual environments. The virtual environments are sometimes called virtual private servers, but they are also known as guests, instances, containers, or emulations.Rudimentary image backup functionality is inherent when using the server virtualization, since each server is akin to having a "folder" stored on a hard drive. When you want to backup a server, you can copy the folder that contains that virtual server. VMware offers VEAM that enhances the backup process immensely.

2. Business Continuity Devices

Business continuity devices exist to help you backup your important data easily and quickly. They're designed for company rather than personal use.

Foster explains that business continuity devices often reside in your data center with your other servers. Their features usually include:

- A snapshot image of your servers taken every 15 minutes, so if a server crashes you're able to quickly restore it to its status of 15 minutes ago.

- The ability to use available bandwidth to copy your data to a secure, off-site data center overnight in case something devastating happens at your site.
- In some cases, the capability to actually perform as a “crashed server” so your users can keep working even if a server crashes.

Generally, the business continuity appliances are sold and maintained by IT consultant firms in your area. The Barracuda is an example of an appliance you can get directly. Foster suggests viewing examples of other devices at www.ConnectWise.net and www.barracudanetworks.com.

Also, contact your local IT consultants to see what business continuity appliances they offer.

3. Online Backups
Online backups are another option for personal computers, workstations, and servers. In this case, the backup takes place over the Internet and the data is stored on the service provider’s servers. Online backup services can backup whatever data you choose.

- **Personal devices:** Many CEOs use online backup for their personal computer. Some of the most common services are Carbonite (www.carbonite.com), Mozy (www.mozy.com), and CrashPlan (www.code42.com). With this type of service, you can opt to backup whatever you’d like, including your accounting software, corporate documents, paperless documents, etc. It’s completely up to you.Foster says that the biggest concern executives have about using online backup is: “Is our data secure?” Most of the companies offer you a method to encrypt your data so that only people you authorize can access it. “Bring up the security question with your online backup provider,” says Foster. “If they tell you they can recover your data for you in the event you lose your password, then that situation isn’t secure enough. You don’t want anyone except you and your team to be able to access your data. If you forget your password then, yes, you won’t ever be able to access your backed up data again, so don’t lose your password.”

- **Workstations and Servers:** Online backup for workstations and servers works the same as it does for individual devices. The added concern for companies who use online backup is how you’ll retrieve your info if you ever suffer a complete loss of data, as in a disaster. Often, performing a complete restore over an Internet connection would take too long, so the service provider should offer you an alternative, such as sending DVDs using overnight shipping. If your provider is within driving distance, you can get your entire set of data even faster.Foster says that he has used an online backup system for years and is very happy with it. But he’s quick to point out that the online backup option is not an image backup. Therefore, you should still backup your workstations every night with an image backup.

4. Cloud Storage (Cloud Backups)
What about cloud options like iCloud, OneDrive, Dropbox, etc. Are they good backup options? Are they secure?

According to Foster, cloud storage options are probably relatively secure, but there’s no way to be sure of servers over which you have no direct control. However, they’re a valid option for both personal computers and work computers. Here’s how he suggests you approach using the cloud as a backup option:

- **Data that is non-sensitive in any way:** You can feel completely confident using any of the “cloud” services, which work well for the purposes of convenience (so you can share between devices and with people outside of your organization) and for “backup” or archival purposes.

- **Data that is slightly sensitive:** If the consequences of a breach would be minimal, feel free to store that information in the cloud. How can you tell? Assume there's a 10 percent chance that the data will be exposed while in the cloud. (In reality, the chance of exposure is probably significantly less than one percent, at least from a technology standpoint.) But be overly cautious, and remember that to take user and employee error into account. For added protection, encrypt the files and data before you put them into the cloud. If you use a service to backup your computer to the cloud, make sure to set the proper settings to encrypt those backups.
- **Data that is highly sensitive:** Cloud storage is not advisable for highly sensitive data. Store this kind of data only on computers over which you have direct control. Don't store any data in the cloud if its loss would be devastating to you, your business, or your customers who trust you with their sensitive information. Period. If you see no way around storing sensitive information in one of the cloud services, then use strong encryption algorithms and strong passwords to encrypt your data before storing it in the cloud. That way, if the data does fall into the wrong hands, it will be more difficult for them to access the data. Just remember that encrypting data is no guarantee that it won't be accessed.

"The key to knowing what to (and what not to) put into the cloud is to categorize your data and consider risks vs. benefits," says Foster. "Cloud storage can save you time, money, and provide added functionality. You just need to make informed decisions about what to store there."

Test, Test, Test!

No matter what technology you choose for your backup strategy — whether you're backing up your personal computer, your workstations, or your server — test it often. Foster has seen too many companies fail when they mistakenly thought they had a backup but didn't, and they suffered a catastrophic loss of data. Therefore, do formal testing and restores at least once per quarter.

The backup error log should be examined daily. Some IT professionals explain daily failed backup errors in their backup log with something like, "Oh, I know why that backup shows it has failed every day. It was caused by the ex-employee's old email account that I haven't had time to delete yet." That's why Foster stresses the importance of deleting the ex-employee's account, or excluding the folder, or doing whatever needs to be done so that the backup log shows "successful" every day. This makes the daily examination of the backup error log much faster.

You can glance to see the "successful" message in only seconds. Reviewing the logs takes much longer when the "backup failed" message appears, because then you have to spend time looking through the entire log to see if something unexpected is "failing." And, more often than not, this "time looking" is not invested. If the log file always has errors, soon nobody will bother to look to see what errors were logged. One day, rather than showing an error of "couldn't back up the ex-employee's email account" changes into the error "I didn't back up the mail server at all" and nobody notices. Resolve conditions that cause the errors so that your log says "Success!" Then, if there is ever an error in the log, it will grab the attention of whoever looks at the backup report.

If all that testing seems too complicated and you're more concerned to know if you even have the most basic of backups, Foster suggests trying this experiment:

- Create and save a simple, non-important file on your network called something like "MyReallyImportantData.doc."
- Wait 24 hours and then delete the file.
- Call IT and say, "Oh, my gosh. I've lost this file. Can you please get it back?" And then start the stopwatch to time how long it takes to get your file back. This is far from a comprehensive test, but it is lots better than not testing at all.

Action Items

- Start using image backup on your own computer — the one that's most important to your daily work. Purchase an external hard drive, throw away the backup software that is shipped with it, and purchase the latest release of Ghost, True Image, or Shadow Protect. Have an IT professional set this up for you so your computer does automatic image backups daily.
- Find out how frequently your organization performs backups, and how frequently your IT department tests the restore procedure.
- Find out where your backup media is stored off site and make sure you feel comfortable with the security of the transport method and location.
- Whatever backup method you use, test it. **Do this today.**

Expert Practices -- Your Disaster Recovery Plan

We see it in the news almost every day, it seems: Natural disasters that underline the importance of creating a solid disaster recovery plan (DRP) for your business.

According to Vistage speaker **Mike Foster**, every business needs one. “A disaster can hit anyone at any time and can include such things as fire, theft, hurricane, long-term power outages, terrorist attacks, hacker attacks … the list is endless. Therefore, your plan needs to allow for the continuation of business in the event that one or more servers, and potentially even an entire office or work location, becomes inoperative for any reason. The DRP includes provisions for rapid transfer to new servers and minimal, if any, downtime for users.”

Whatever you do, please don’t think that your business is immune from some sort of disaster. Every business is at risk.

Also realize that one disaster, even a small one, has the potential to close your community and your business indefinitely. Taking some time to plan now will save you a great deal of headaches and frustration in the long-term. Additionally, Foster explains that planning now will help you:

- **Reduce the impact of the disaster.** If you have a plan in place for what happens when disaster strikes, you can take proactive measures. You’ll have a clear step-by-step game plan for what needs to be done, when, and by whom.
- **Continue to work with your vendors and suppliers while you’re recovering.** No man (or woman) is an island. Your vendors will be key contacts post-disaster. Put them in your plan so you’ll have a clear idea of how they can help you recover.
- **Resume critical business functions.** Trying to plan after the fact is a difficult process. Not only are you dealing with immediate loss, but you’re also not in a clear state of mind. Knowing what you’ll do before something happens saves precious time later so you’re up and running sooner.
- **Ensure your business will survive.** Just as you likely have a business plan to guide your company’s growth, your disaster plan will guide your recovery efforts so you’ll know you can overcome whatever faces you.
- **Provide safety for your workers.** As an employer, your employees’ safety is your responsibility. Disasters pay no attention to the clock and can strike any time of day. If one happens while your employees are on the clock, you want to ensure you’ve taken their safety into consideration.
- **Keep customers now and in the future.** People only want to do business with companies they perceive as rock solid — someone who’ll be there in the future, no matter what happens. When your customers know you’re prepared for anything, they feel more comfortable doing business with you.
- **Receive insurance discounts.** Tell your insurance agent that you have a disaster plan in place and be prepared to show documentation of your plan. Some companies may be able to provide you a discount on your premiums.

Plan Wisely

“Your biggest investment in creating a DRP is your time,” says Foster. “Many of the preparation tasks do not

cost much money, but planning does take time. However, the time you do invest will pay off, if and when a disaster should strike."

Foster suggests that rather than plan for every single thing that could happen, you should try to anticipate the worst-case scenario and plan for that. For example, if you live and work in Minnesota, you don't have to plan for a hurricane. But you should plan for flooding, blizzards, tornadoes, technology breakdowns and theft.

Start with the most likely risks first. Are you near a river that routinely floods its banks? Do you live in California where mudslides, earthquakes, and wildfires are common? Is your business located in tornado alley? Look back at what has happened in your area, even if the event didn't directly affect you. At this point, you're simply trying to get a good idea of the possibilities.

Additionally, consider smaller disasters too. For example, a simple server crash can disrupt your business for days if you don't have an off-site backup and a recovery plan in place.

Examine the risks in the following list to determine what is likely to occur in your area.

- Nature
    - Wildfire
    - Earthquake
    - Flood
    - Hurricane
    - Tornadoes
    - Other High Winds
    - Lightning Strike
    - Pandemic
- Hazardous Materials Spill
- Technology Related
    - Aging Computers Failing
    - Denial of Service attack (This means you cannot send data in or out of your office; e-mail, web browsing, and all other internet activity stops.)
    - Data theft
    - Deleted data (Either intentional or accidental.)
- Someone else's disaster affecting you
    - Disaster with a key supplier, distributor, internet service provider, phones (mobile, VoIP, or land line), shipping partner, payroll firm, or utility provider
    - Pipeline explosions and burst dams
    - Blocked routes
    - Rail/Waterway/Highway/Air disaster
    - Nearby fire, explosion, or any other disaster
- Crime

Know Your Metrics

As you create your DRP, Foster recommends that you make decisions about your **recovery time objective** (RTO) and **recovery point objective** (RPO).

Your RTO specifications are the lengths of time you plan to tolerate being down for specific levels of service. For example, your RTO for your email server might be one hour, and your RTO for the accounting system might be a single day.

Next, define your RPO, which is the amount of data you'd allow to be lost forever from the system. If you perform backups every six hours, and the crash happens five hours after the most recent backup, then the work done during those five hours will be lost when you restore from backup. In this example, if you're meeting your RPO objective, then the RPO is six hours since you've chosen to backup every six hours.

"The shorter the RTO and RPO times, the more expensive the DRP solution will cost to implement," says Foster. "At the same time, long RTO and RPO times can cost the organization large sums of money in the event of a disaster."

Spend Wisely

The key, explains Foster, is to balance the cost of implementing the DRP with your needs. He offers the following simple way to determine a rough budget for your DRP: **Calculate the money you will lose when your company is without a network and then multiply the costs times the percentage of likelihood of that disaster occurring.** This gives you a rough budget for your DRP. To tune that amount, you can calculate different costs and likelihoods for being down an hour, a day, and a week. This gives you not only a more accurate amount, but also a better idea of how quickly the network needs to be up and running again.

With all this said, don't go overboard with your DRP, but invest enough to protect yourself appropriately. According to Foster, when it comes to disaster planning for your company's data, you have several options and levels of backup servers. As you move up the scale, you will invest more money in your DRP, and at the same time, you will experience less downtime in the event of a disaster.

Some options for the DRP that Foster recommends include:

- **Bare Minimum Protection.** Keep a list of specifications for new servers you'll need in case you lose your existing servers. Make lists of the default builds of workstations and servers. Be sure to store these lists somewhere else, in addition to on the network. That way, if the network is unavailable, you'll still have access to the lists.
- **Low to Mid-Level Protection.** There are appliances available on the market that make image backups of your servers at regular intervals and offload the data to a central data center throughout the day. If one of your servers dies, the appliance can virtually take over the work of that server until you fix the hardware. Once your server hardware is functioning again, the appliance can restore the image rapidly. In the event the appliance is destroyed, the manufacturer will ship you a new appliance that is loaded with the most recent data you uploaded over the Internet — hopefully, less than a day old. The pricing is very aggressive and these solutions are worth considering for small- to medium-sized organizations.

- **Mid to High-Level Protection.** Purchase “cold standby” servers and keep them off site. Then, if there is a disaster, you just move those servers on site, restore your backups, and start up again. With this type of DRP, you can potentially be up and running again within the same day the disaster strikes. Your team will want to practice this restore process at least yearly. The good news is that, to save money, some solutions allow you to have a single standby server that can take on the load of more than one of your production servers in the event of a disaster. This technology has come about in recent years thanks to the implementation of server virtualization technology, which also vastly simplifies the process of moving your current servers to the standby servers.
- **Highest-Level Protection.** If being down for one day is unacceptable for you, then you’ll need a more advanced DRP. In that case, you have what’s called collocation. That’s when you have two sets of servers in more than one geographic location. This can be very expensive unless you already have two locations for your business connected with a high-speed data link. Then, if any or all of your servers go down, the other servers just take over. You may choose a relatively low-risk place for your second servers, such as the middle of Arizona. Other organizations that have offices in multiple locations often choose to use a secure room at a second office to house the standby servers.

When it comes to spending, do the most important preventive measures first, and then move on to the others as time and money permits. Remember the following “non-IT” steps too. You may focus too much on the technology and fail to address other important items that will indirectly affect IT. Foster details the following “must do’s,” “should do’s,” and “can do’s.”

1. Must Do Items

- Keep a backup plan for your:
    - Data
    - Machinery
    - Key personnel
    - Suppliers
    - Electricity
    - Communications
- Inspect and maintain equipment regularly.
- Install emergency sensors and alarms.
- Install fire extinguishers.
- Install emergency electrical generators.
- Protect your IT equipment and check into and/or activate:
    - Off-site backups
    - Cold standby servers
    - Collocated servers
    - Redundant routers, firewalls, and internet connections

2. Should Do Items

- Get yourself and every employee trained in CPR and basic first aid.
- Have general safety training for staff.

- Have fire and safety inspection by the local fire department and other professionals.

3. Can Do Items (if applicable)

- Install automatic shut-offs for key equipment.
- Install pumps in water prone areas.
- Invest in N95 respirator masks for your staff. These masks are designed to protect the wearer from airborne diseases.
- Build levees to protect your facility from flooding and/or to enclose hazardous materials.

Testing is Crucial

"You must test your disaster recovery plan regularly," says Foster. He recalls performing a security review and being told by the CEO: "We have all this disaster recovery planning stuff in place, and we're paying a company to help us with it. But for us to test it, they want to charge us $10,000, so we've never tested it."

To Foster, that's an unacceptable situation. He advises setting up yearly testing as part of the original agreement. Establish the testing plan to be thorough and recurring. Otherwise, if your plan isn't tested regularly, you have no idea if it will actually work should the need arise.

The Biggest Overlooked Disaster

Finally, realize that if your sole IT professional, or any key member of your IT team, gets seriously ill or injured and can't come to work for an extended length of time, that's a disaster too. You need to plan for such a scenario. Therefore, Foster recommends you have great documentation of your system, including, but not limited to, the following:

- Network diagram
- Device inventory
- Hardware and media assets
- Internet and WAN connectivity
- Administrative passwords
- Data flow diagram
- Description of business needs relating to the security of data, including firewall and router filtering rules
- List of who has access to what
- List of vendors, service providers, consultants, and support with complete contact information
- Server and workstation configurations, including
    - IP Addresses
    - Information on remote offices and/or users
- Routine tasks such as resetting forgotten user passwords
- Backup / Restore procedures
- RAID array procedures
- SAN (Storage Area Network)
- Inventory of software applications

As a side note, collecting all this information is in line with IT best practices. Should your IT professional leave or be unable to work for any reason, any qualified IT professional can now walk in and take over without having to start from scratch.

Remember, losing your IT professionals could result in a loss that could be just as great as what would occur in the event of a natural disaster. So have a plan for everything. While it's hoped that you'll never need to enact your plan, you definitely need to have one, just in case.

Action Items

- If you have no firm DRP in place, use the next three months to begin planning one.
- During this planning phase, determine your risks and budget and seek out options for your plan's deployment.
- Determine a realistic end date for your DRP to be complete. If you never set a date, then chances are you'll find yourself without a DRP for many more years to come, and that's a dangerous place to be — especially if you aren't using server and workstation virtualization technology yet.
- If you haven't already, find a provider in your area that understands virtualization and is experienced enough to set up virtualization for different companies at least once a week. Almost invariably, companies that complain about problems with virtualization can trace their problems back to misconfiguration by whoever implemented the visualization. Leveraging virtualization technology can save you large amounts of money and provide increased functionality.

Expert Practices -- How to Effectively Outsource IT Services

Many companies outsource their IT needs and services. That is, they don't have any internal IT staff and bring in outsiders to handle that aspect of their company. Depending on the nature and size of your company, outsourcing your IT may be a good decision. If you have a dedicated IT team on staff, chances are good that they're extremely busy, so bringing in some outside help to assist your main IT staff can be a great idea.

According to Vistage speaker **Mike Foster**, the key to making the outsourced IT relationship work is to really know the company you're working with. "Check them out and make sure it's a company you feel confident being supported by," he advises. "Most managed service providers advertise big services, but many don't deliver."

Foster also offers some "pros" and "cons" of outsourced IT support that every CEO should be aware of.

The Cons

When your organization outsources IT support without the appropriate checks and balances, the tactic of "put out the technology fires but don't *prevent* the fires" can get out of control. Foster explains the vicious cycle as follows:

1. You experience a problem with some technology in your company and you contact your outside support company to come put out the fire by fixing the visible problem.
2. They respond, solving the problem you called about.
3. You pay the bill, whether it's hourly or part of a service agreement.
4. Since the root cause was never addressed, the fire ignites again later.
5. Return to step 1 above and repeat forever.

Many companies really appreciate their IT vendor for being responsive and fixing all the problems. Unfortunately, they're oblivious to the fact that the underlying problem is still there. Some outsourced companies are oblivious to the underlying problem, too; they feel that their mission is simply to put out fires.

"Putting out fires instead of addressing the root problems is especially expensive when you take into account the loss of user productivity, the damage to your brand, and other intangible costs related to the frustrations with malfunctioning technology," explains Foster.

So if you happen to be one of the many companies that outsource IT, Foster has a special assignment for you. Call your IT service provider and say, "I know we call you to come in and fix whatever's broken, but we'd like you to come in for a little extra time to advise us on proactive steps that we should take now in order to prevent future problems — especially problems like we've been having recently."

Having outsourced IT providers fix what's wrong without fixing the root of the problem is in *their* best interest, not *yours*. It guarantees they'll have a steady amount of work from you. However, you're better off having them come in, tighten up all the hatches, and get things running right.

Another problem is that too many organizations hire outsourced IT companies and pay them by the hour, explains Foster. But think about it. If you pay an hourly rate, what is the IT company incentivized to do? If you said, "take longer," then you're exactly right.

Not only will they take longer, but outsourced IT companies can send inexperienced staff members to your location to respond to your requests. If these inexperienced people aren't familiar with whatever you want them to do, then they'll spend time educating themselves. Eventually, they will likely solve the IT problem you wanted them to fix — but you just paid an hourly rate while they educated themselves.

For consultants confident in their experience and skillset, that confidence removes the fear they would otherwise feel about "moving to a flat fee arrangement." They will be happy to comply. If they are fearful of moving to a "flat fee" model, it may be because they aren't confident in their technology skills, or in their communication skills. Communication skills are important in order to specify from the very beginning exactly what they are and are not going to deliver for the flat fee. Additionally, if you start changing the scope of the project, be prepared for them to tell you how that change is going to affect the flat fee to which you agreed.

"Utilize outsourced IT companies that have the expertise on staff to handle the projects you want to outsource," says Foster. "If your business is in a rural area with few IT professional companies to choose from, then discuss with them ahead of time how you don't intend to pay them while they increase their own knowledge to a level where they can help you."

To save money and receive better service when you utilize services from an outsourced IT support company, Foster says that you should first define the scope of the work. Then, leave it up to them to provide you with a flat fee for the work. That way, they're incentivized to do the best job they can and also use their time wisely.

The Pros

The biggest pro of using an outsourced IT provider is the level of expertise you can get. As Foster explains, "Think about it this way: How would you feel if you walked into the hospital and the receptionist said to you, 'Good morning. We'd like to introduce you to Dr. Smith. He's our resident cardiologist. He's also our resident brain surgeon, our resident neurologist, our resident OB/GYN doctor, our resident … ' If you were to hear that, would you think this doctor is really qualified in anything? No way!"

In the IT field, it used to be that one person could be an expert in everything technology related. But because technology has expanded so much over the years, that's no longer the case. Even so, many IT professionals still think it's their responsibility to do everything in the IT department. Often, this can cause problems. That's when you need to bring in outside help, says Foster. "Here's where an outsourced IT company can be most useful because they can have many people on staff, each with his or her own unique expertise."

Additionally, outsourced IT professionals see many different businesses and often recognize problems early on, before they have a chance to damage your organization. "Also consider that when you outsource your IT needs, you don't have to send people to expensive schools and long training programs so they can learn how to configure some device that will only need to be configured once," says Foster.

Even better, some IT outsource firms have alliances with vendors that can get you special pricing on hardware and software. Finally, should your own IT professionals move on or become ill, it would be nice to have a solid outsourced IT firm to fall back on during emergencies.

Therefore, be sure you support your IT professional, especially if he or she says to you, "We're getting ready to implement SharePoint. It'd be really nice to have someone who is experienced with SharePoint to help with the initial deployment to make sure everything goes smoothly and that the foundation is solid." Make it okay for your IT professionals to bring someone else in if they want or need to. That's when you're using IT outsource providers in the most effective way: You're relying on the specific expertise of someone to help your company get over a hump or take care of a challenge.

Action Items

- Even if you have an IT staff, investigate some IT outsourced firms specializing in areas where your IT team would appreciate assistance.
- Call the IT firms and schedule meetings to discover how they can assist you with your IT needs.
- Renegotiate with your providers so they start billing you a flat fee based on accomplishing specific tasks and projects. Tell them you don't want to pay them by the hour ever again. If they refuse, and you like working with them, then at the very least start having them provide you with a "will not exceed" price and completion date from now on. If they still refuse, then tell them this four letter word, "Next!" And go find yourself a different provider with more confidence in their own abilities.

Expert Practices -- 10 Steps to Control Technology Spending

Technology spending can get out of control. And, according to Vistage speaker **Mike Foster**, neither executives nor their in-house and/or outsourced IT professionals necessarily know where to cut costs.

To help busy executives rein in costs, Foster offers the 10 steps to help you grab the reins of technology spending:

1. Don't buy storage with massive capacity you're not likely to need — especially if it adds too much to the price. You may indeed need a great deal of storage if you store a lot of drawings, photographs, videos, scanned images from when you went paperless, etc. But otherwise, why purchase a SAN that can hold 500 terabytes when you really only need 25? It's the same with workstations. For workstations that run Microsoft Office and simple programs, investing in a 64-gigabyte SSD solid state drive will help the computer run faster and stay more reliable than using a three-terabyte mechanical hard drive with a spindle.

2. Think twice before paying for extended warranties. Paying for "on site emergency responses" may be important in some circumstances where equipment is mission critical. While those warranties are justifiable for servers, purchasing expensive warranties for workstations can reduce your ROI. Unless the computer is in an environment that's dusty or caustic in some way, workstations are more likely to become outdated before they fail. In other words, be sure the risks are high enough to justify the cost of the warranties.

3. Shop around every year to find the best deal on connections between your offices and the Internet (i.e., bandwidth). Prices often fall drastically in a short period of time. It seems like the large carriers are always offering a "special deal" to upgrade to their "new faster service." However, there's no need to pay for a 100 mbps connection to the Internet when you never exceed 30 mbps of traffic.

One thing to pay attention to is the fact that some services use asynchronous communications where inbound traffic comes much faster than the traffic leaving your office. Normally that's fine, but using VoIP (Voice over IP) technology demands high bandwidth in both directions.Additionally, any offices with servers that are accessed by other offices need to have a high speed uplink, too. Otherwise the remote offices will experience a delay in the data they expect to receive from your server. If that's the case, it may be more beneficial for you to host that server in a data center. Data centers have high-speed synchronous communications (in addition to all of the other benefits data centers provide).

4. Use the full power of the hardware and software you already own. Most businesses already own hardware and applications that can perform more functions than you'll ever need. And most everyone wants to find happiness in life by getting rid of old frustrating technology. That sometimes makes us over-eager to adopt the "latest and greatest" solution that we decide "will finally make all our problems go away." Beware of the sales pitch! Foster has seen many companies on the third version of their ERP (enterprise resource planning) software but still using only the functionality they had in the previous two versions. Often, executives and even IT professionals have unreasonable expectations of what technology can do. It's often better, and more economical, to utilize what you already invested in.

5. Perform preventive maintenance. As with many other things in life, performing preventive maintenance can save you a lot of wasted time and money (not to mention headaches). Unfortunately, most companies are so overwhelmed with the big IT tasks that they fail to remember to maintain what they have. Every so often, blow out dusty computers. Replace power supplies when their fan starts making noise. Change out old

keyboards if their keys stick. You'll find that when you take some time to address the little things, you prevent them from becoming big things later.

6. Use server virtualization to save money on servers. "Server virtualization" is when you use fewer physical computer boxes that "behave as if" they are three, five, or even more physical servers. In technological language, the physical servers host other guest operating systems.

7. Adopt workstation virtualization. Workstation virtualization is finally becoming common, even though most everyone has used server virtualization for years. If you're one of the companies that hasn't yet adopted workstation virtualization, then explore the opportunity immediately!An important caveat: If the workstation virtualization is configured improperly, you'll experience nightmares. In fact, those companies that did make the switch and didn't like it were often victims of inexperienced installers. Find a provider that sets up workstation virtualization at three companies each week. You'll have a better outcome.

Also, don't expect your internal IT professionals to be familiar with such a specialized task, unless they truly are. There are so many big benefits to moving to workstation virtualization that, although you pay extra on the front-end, will save you tons of money in the long run. (One of the ways is reducing expensive ongoing tasks such as patching, backup, support, reloading and building workstation configurations.)

Workstation virtualization comes in many forms. One way is when programs all run on a single server, with the computers merely acting as screens and keyboards. Another way involves streaming applications to the workstations as necessary. Proper planning is imperative. You may choose to start first with your remote users. The users can be using Windows, a Mac, a tablet, or just about anything since programs can run on the server and the device can act as a screen and keyboard. Beware that trying to use small screens, such as the screen on a smartphone, may provide a less than optimal experience for your users. But using larger screens can be just fine.

Workstation virtualization can solve a myriad of problems — probably more than you can imagine — on which organizations often spend a great deal of money (or choose not to implement because of the cost). For example, just by moving to workstation virtualization, there are business continuity and disaster recovery features "built in" for no additional expense.

8. Consider buying refurbished equipment. Don't be afraid of allowing your IT professionals to buy refurbished equipment and to sell your old equipment on auction sites. There are security concerns that need to be addressed, but other than that, reusing equipment is a lot better than having tons of it stored in offices and storerooms around the world. Even manufacturers sell "previously owned" refurbished equipment backed by a warranty — and it's often more than adequate for your needs.

Additionally, it's sometimes advantageous to buy an older model of a computer. (For example, it was okay to buy the older Microsoft Surface Pro computer at a 50 percent discount rather than pay full price for the newer Microsoft Surface Pro 2. There were so few enhancements in the Pro 2 model that most users would never notice the difference.)

9. Don't pay outsourced IT by the hour. Too many organizations hire outsourced IT companies and pay them by the hour. If you pay an hourly rate, the IT services company is actually being incentivized to take longer. Not only *will* they take longer, but they'll often send inexperienced staff members to your location to respond to your requests. If the inexperienced people aren't already familiar with what you need, then you're effectively paying an hourly rate to educate them.

Here's how to save money and receive better service: When you utilize services from an outsourced IT support company, clearly define the scope of the work. Then, leave it up to them to provide you with a flat fee for the work. That way, they're incentivized to do the best job they can and also use their time wisely.

10. Finally, **stop killing alligators and just drain the swamp**. Too many IT professionals run around like fire fighters rather than just fixing the root of problems. Why? Because that's what executives have trained IT to do. "Email is down? … I'll fix it." "You can't open this document your colleague emailed you? … I'll fix it." "You're getting an error message when you try to print? … I'll fix it."

By focusing on the problems, IT becomes the knight in shining armor. However, the mark of great IT professionals is when you never see them and everything works the way it's supposed to. But that only happens when IT team members know how to prioritize their tasks.It's a matter of changing perspective. Just because you haven't seen your IT professional in three days doesn't mean that he or she is playing solitaire all day. Your IT professional is probably very busy, especially if everything is working right. And that's what you're really paying for anyway. So from now on, when an IT professional solves a problem, instead of saying "Good job for fixing that," ask "What could you have done to prevent this?" That will refocus IT on what is most important — preventing problems before they even happen. In other words, they'll have drained the swamp, causing the alligators to leave.

Action Items

- Sit down with your IT professionals and evaluate all your IT expenses.
- Ensure that you're only paying for the services you need and that you're using what you have effectively.
- Discuss ways to keep projects on budget and on time with your IT professionals.
- Shop around for the best deals on services, hardware, and software.

Expert Practices -- Updating and Patching Operating Systems and Applications

To keep your computers and network safe, you need to regularly patch and update your operating systems and your applications. Why? According to Vistage speaker **Mike Foster**, “Attackers look for common weak spots on your network, and the two most common vulnerabilities are unpatched operating systems, such as Windows, and unpatched applications, such as MS Office, Adobe Reader, Flash, and Java. That’s why you want to keep your operating systems patched and your applications patched and upgraded to the most recent version.”

At this point many executives ask, “What are patches?” Foster explains that some people call patches by another name: updates. There’s generally no charge for patches, and they’re usually designed to fix some kind of “chink in the armor” related to a security issue with the program. Patches are not ever made “just for fun.” They fix very important vulnerabilities and/or make important changes that will keep your systems from crashing when you need them the most. Unfortunately, patches are often neglected and, if something bad happens, companies wish they could somehow “go back in time” to apply the patches they hadn’t.

While applying the patches seems like such an easy thing to do (and for very small networks it generally is simple), patching is actually a complicated matter, says Foster. Here’s why:

- First, as you update, you need to pay attention to whether something is a feature update or a security update. Feature updates simply add new functionality to a program. So it doesn’t matter, from a security standpoint anyway, whether you install feature updates or not. Foster advises that you keep your focus on the security updates and patches. Without the proper security patches on your applications, your computer is more vulnerable to a hacker attack.
- Second, you can’t just patch one or the other — either the operating systems or the applications. You must patch both. Why? “Think of it this way: If you lock your doors, the thieves may try to come in through the windows,” says Foster. “In other words, if the hackers can’t get in through the operating system vulnerabilities, then they will attempt to exploit your applications. That’s why both need to be patched.”

In fact, attackers have learned that one of the easiest and most successful ways to successfully take control of a network is to launch attacks against vulnerable programs on your systems. Many viruses and other malware exploit vulnerabilities in applications. Are all of your patches current for applications such as Adobe Acrobat, Flash, Java, Microsoft Office, etc.? And do you have the latest versions of those applications? Do your IT professionals have the tools they need to monitor and manage the versions of Reader, Flash, and Java?

When to Patch Your Operating Systems and Applications

It’s best to make sure all users have all “high priority” and “critical” patches and updates tested and applied within hours of their release. If you elect not to apply certain patches right away, Foster advises that you establish another control to mitigate or eliminate the risk of not having the patches in place. The sooner you test and apply patches, the sooner your systems will be protected against the vulnerabilities those patches fix.

Choosing aggressive patch management helps to protect you against attacks. Even though operating systems patches are used by a great number of users in the world, be sure to act aggressively rather than wait four weeks to “see if anyone else in the world has problems.”

Important application patches that affect security and availability need to be deployed as soon as reasonably possible, preferably no later than a day after release. Within hours is even better, and days are better than weeks. Realize, too, that attackers often exploit applications before the vendor has issued a patch to prevent the exploit. These attacks are referred to as zero-day exploits.

The Patching Dilemma

IT professionals, both in-house and outsourced, have a valid reason for being averse to patching. After all, the IT professionals are already very busy, and a patch might disrupt the stability of the network. They certainly don't want to do something to the network that could cause problems.

IT professionals understand the often grave dangers of not having patches in place, but to them it may seem easier to skip the application of patches and deal with any possible repercussions (from the patches not being applied) later.

However, by not applying patches within 48 hours of release, IT professionals are taking a huge risk with your company's security. You may be okay with that, considering the potential problems with patch application; the key is that this is the executive's informed decision. This topic is too important for your IT professional to decide on his or her own.

Foster goes on to explain a common irony today: In most cases, patches to user computers (a.k.a., workstations, as opposed to servers) rarely cause any problems. Patch application to servers usually goes smoothly too, but sometimes your IT professionals will want to be right there providing TLC to the server as it is patched. For larger networks, being there becomes essential.

Of course, once they realize the importance of needing to apply patches to the operating systems and applications, most executives agree that it's something that must be done. So how can they get their IT team on board? Here's what Foster suggests:

Executives need to give their IT team a "get out of jail free" card. In other words, if the patch causes something to not work properly, you won't blame or attack the IT department. This will reduce the stress the IT professionals feel so they're not "under the gun." But, before you give your IT team this free reign, executives need to rigidly enforce three stipulations.

1. The patches are thoroughly tested before deployment. (See "Testing of Patches" later in this module.)
2. The IT department must use staged deployment. (See "Staged Deployment" later in this module.)
3. The IT department must have an easy rollback method. (See "Testing of Patches" later in this module.)

Upgrades are Just as Vital

Additionally, make sure you're only using recent operating systems. Operating systems like XP and Vista — and especially anything older than these — are outdated. If you use them, upgrade them as soon as possible. Of course, executives have a valid reason to be averse to upgrading operating systems from, for example, the version of Windows they bought five years ago to what's currently available. However, unless you stay current with operating systems and applications, or at least establish compensating controls, you are more vulnerable to attack. That's another reason why patches are so important.

So please get computers with those old operating systems off your network. According to Foster, those old computers have vulnerabilities for which Microsoft no longer provides patches. Use those older computers for specific functions if you have to, but do not connect them to your network. If they *are* going to be on the network, they need to be isolated. For example, the computer may control some expensive and/or important

piece of machinery in your company. The vendor of the device may not support new operating systems or may want to charge a huge sum of money to upgrade you to their latest application. If that's the case, don't change that particular computer. But be sure to remove it from the network.

If you need to get information over to one of those machines, copy the information onto a CD or a memory stick and take it there using what Foster refers to as "Sneakernet." If you're in a situation where you need the older machines connected to your network, then there are other alternatives that sometimes work, such as running the older operating system in a virtual machine hosted on a secure machine using a current operating system and a tool such as VMware from www.VMware.com. VMware by itself doesn't guarantee security, but it can be a big step in the right direction. Of course, you don't want to interrupt your users' ability to get their work done, yet at the same time, you have to make sure you're secure.

Did you know that your network may become infected when your users visit websites? "Drive-by" downloads are a major source of attacks. Microsoft makes major security improvements with each release of Windows and each release of Windows Server. More recent versions of Microsoft's browser Internet Explorer (IE) are significantly more secure that the previous version. If you're going to use IE, use the newest IE supported by your operating system.

Realize, too, that Microsoft, as well as other operating system vendors, generally stops focusing on patches to older versions of their operating systems. Eventually, the vendors drop support all together. Sometimes upgrading to the next operating systems version can create unstable systems and unexpected results, especially in relating to the other systems in your environment. Even though you may not necessarily move immediately to new operating systems, in order to continue to protect your organization's network, strongly consider upgrading to the latest version within less than six months after release. Sooner is better from the standpoint of security unless the new version has unexpected security flaws. It's important to emphasize: Upgrades to the latest version should not be confused with updates or patches. Updates and patches need to be installed much sooner.

But upgrades aren't just for operating systems. More often than ever, attackers are targeting older versions of applications. Examples of applications that need to be current (some of which offer free upgrades) include Adobe Reader, Adobe Flash, Java, Microsoft Office, etc. If your organization uses old versions of applications, you have a much larger exposure to attacks. Computer application vendors release upgrades to new versions, often every year.

With Microsoft now offering the model of "renting Microsoft Office" through their Office 365 program, there shouldn't be any excuse for not spending money to upgrade to the latest version of Microsoft Office, especially since there isn't a fee for the upgrades. The upgrades are included. If you are frugal and work the math, you may or may not find that, in your situation, purchasing Office outright rather than via subscription is less expensive. However, you must remain cognizant of the fact that you need to pay for the upgrade the next time a new version of Office is released in order to maintain the highest level of security that Microsoft is offering.

Have an Inventory of Applications

Your organization's IT professionals need to create a list of applications; otherwise, they don't know what needs to be patched. They won't patch an application if they don't even realize the application exists on your network. That oversight may be the one that costs you your businesses' reputation.

Therefore, keep a current inventory of applications and what users and/or machines have access. Remember, too, the applications installed everywhere from the servers to users' portable devices such as laptops. Even home computers need to be inventoried and patched if those computers are used to access the company network.

Don't go overboard on the inventory documentation — some reports can be hundreds of pages long, and those aren't useful. A thorough list will include the version number and patch level of the applications. Many enumeration tools such as endpoint protection tools, host based IDS/IPS, patching tools, and so on will provide you with a detailed inventory of all of your applications.

If any applications are unnecessary for business purposes, they should be removed from all computers in order to reduce your organization's security exposure. The added benefit? You won't need to patch those applications since they will no longer exist.

Users installing their own programs can severely compromise the security of your systems. Never allow users to install their own applications. Reconfigure your group policy and user systems to enforce this. IT professionals should install applications when necessary.

Use Central Management Tools to Make Patching Easier and More Reliable

Attackers constantly probe operating systems and applications to find vulnerabilities to breach your network, steal information, and control your machines, among other activities. Vendors release patches on a regular basis, and the patches need to be monitored daily. Centrally manage this process instead of relying on users to take care of "automatic updates" on their own.

Use Microsoft WSUS, Microsoft SCCM or System Center Essentials to apply operating systems patches. There are numerous other commercially available patch management tool alternatives too. Another option is subscribing to managed services from an IT services firm to centrally manage and monitor patch status across your network. But, as Foster explains, "You better have someone who knows what they are looking for manage your managed services provider (MSP). There are benefits to an MSP not applying patches, so they may not actually apply all of the patches they tell you they are. They often feel this is 'for your own good' that you don't have the patches. Here again, if and when to apply patches is a decision you need to make, not them."

Application deployment tools, sometimes referred to as application streaming, work even better than simply deploying patches to applications that already exist on individual computers. With application deployment, each time a user wants to use a program, that program is deployed from a central computer to the user's workstations. The program is updated centrally, so each time it's deployed the program is up to date.

Testing of Patches

Deploying operating systems and applications patches directly into your production network can cause unexpected problems. Rather than wait to deploy the patches — since waiting will potentially put your organization in a precarious and dangerous security position — test the patches in a quality assurance (QA) test environment.

Start testing immediately after the patch is released. Microsoft generally releases patches on the second Tuesday of every month, commonly known as "Patch Tuesday." Your IT Professionals can plan ahead to keep their schedules open for that time. Desktop and server virtualization can help IT with the testing process by providing a method to run server and workstation configurations on a single piece of hardware for testing. If you have a very small company, that QA environment may simply be one computer on which every program your organization uses is installed. Larger organizations will have a full-fledged QA environment.

During the QA testing, carefully check all of your own applications that are not "main stream" applications since you may be a member of a small number of entities that are testing the operating systems patch with that particular application.

Additionally, the IT department, or outsourced IT firm (especially if the firm provides "Managed Services") must test the patches in a similar environment. In other words, an IT professional can't install and test the patch on

his or her own computer, see that it works, and then expect it to work just as well in the business environment. Similarly, an outsourced IT service provider can't test the patch at one company and assume it'll be fine at another company.

Finally, your IT professional should have a rollback plan. Suppose the patch gets applied to five machines and then some program starts to exhibit buggy behavior. The IT department must have a quick and easy way to remove the patch and roll things back to how they were before the patch was applied. The IT team can then analyze and fix the problem, and reapply the patch later.

Deploy Patches in Stages

So, if there are problems, how can you catch them early? Foster recommends rolling out the patches in stages. For example, if your network has:

- **Less than 10 users:** With such a small network, you might decide to be sloppy. Often, you'll get away with it. But it sometimes fails, so you may want to move to the next paragraph. If not, then keep good backups and set the computers to run automatic updates. Especially after the second Tuesday of every month, check each computer to see if it reports that it's up to date with Microsoft's latest patches simply by choosing the "check for updates" option. Use the appropriate vendor's "check for updates" features in Reader and Java too. If you get a message about one of them being out of date, the safest thing to do is go to the source site and download the latest version. If you click a link in an email message saying, for example, "Click here to update your version of Flash," there is a very good chance that the link will redirect you to a bogus site that contains malicious software.
- **Between 10 and 100 users:** Use a centrally managed patch solution such as Microsoft's free WSUS or one of the paid commercial tools (which tend work better than WSUS). A restriction of WSUS is that it doesn't patch applications such as Reader, Flash, and Java. Alternatively, consider using an outsourced IT services company to provide "managed services" that include patching and monitoring your computers. It is essential that you partner with an independent third party who provides oversight of your network and the MSP's success on your specific network.
- **100 or more computers:** Implement a successful change management process. QA is one of the biggest parts of the process. If a patch is released prematurely and causes a problem in your environment, it will affect a great number of users. Schedule the change management to be the top priority, akin to "dial 911" priority, right after the second Tuesday of every month. Test immediately in the QA environment. If you don't have a QA environment, then designate specific computers as "the test computers" that receive the patches before anyone else. Document your change management procedures, requirements, and approval process.For even larger entities, establish and enforce policies and procedures to document all modifications, including fixes, to the applications, hardware, network configuration, and all other modifications. Include the date, location, name of the person who approved the change, person making the changes, the quality assessment process, testing, effects on productivity and security, and follow-up up to ensure maintained integrity.

Operating System and Application Patches at Home

In Foster's experience, executives often want to apply the information found in this module at home, as well. And it is important to keep your home machines protected to protect yourself, your family, and even your office if you use your home computer to work remotely. For home computers, if you have Windows 7, just type "check for updates" in the window that pops up just above the start button. If you have Windows 8, select the "settings" charm, select "change PC settings" in the bottom right, and then select "update and recovery." (When newer operating systems are released, they'll have similar options.) For Macs, with OSX configured as it is today, simply click on the apple icon on the top-left corner of your screen and choose the option that indicates that you want to check for updates.

The high-priority patches — the ones that appear at the top of your results screen labeled as “high priority” — are the only ones you need to be concerned with at this point. The high-priority updates are very important, because they either fix a security problem that Microsoft knows about, or they fix something else important that’s broken in Windows, which could cause your system to malfunction.

After you install the priority updates, you need to scan for updates again. Why? Sometimes the updates need updating. So yes, you may have to update your updates. While the extra step may seem redundant, it’s well worth it to keep your computers safe. This applies to both Windows and Mac machines.

Action Items

- Sit down with your IT professionals and discuss your patching strategies for operating systems and applications. The primary topic should be how aggressive they are with the patches. Do they finish applying patches within 48 hours? Discuss the pros and cons. Strongly consider giving them the approval that you won’t hold them accountable if a patch causes a problem as long as they perform the steps you require them to perform. All of these steps are described in detail above:
    - Test the patches first
    - Deploy the patches via staged deployment
    - Have a rollback procedure in case of problems
- Know that qualified, independent third-party security specialists can come in and assess the patch situation because many viruses will actually cloak the patch status such that your IT professionals cannot see the actual patch status. You need the third-party assessments in addition to what your managed service provider and/or internal IT professionals are checking. Your internal IT pros will welcome an extra set of eyes. They realize how essential patches are to keep your system secure and to keep your system running free of bugs. This check should be part of your annual IT review that will be performed by the qualified IT reviewer who has earned their CISSP, CEH, and CSA certifications.
- Also, your organization’s IT professionals need to create an inventory of applications installed anywhere on any machine or device that connects to your network at any point, including home machines and portable devices if applicable. Unless they identify all of your applications, they will not be able to patch all of them. The inventory (and it’s a good idea for you to review the list in case you see any applications that seem absurd to you) should be limited to a simple list of the applications. If you receive a report that’s more than a few pages long, you won’t have time to review it.

Expert Practices -- Protecting Your Network from Remote Worker Security Risks

These days, it's common for companies to have remote workers and/or employees who travel extensively. Having team members work remotely has many benefits, and having employees who travel to client locations does wonders for relationship building. However, Vistage speaker **Mike Foster** reminds us that there are also some definite security concerns when you allow people to remotely connect to your network.

Here's a simple example he shares: Consider for a moment that you have an employee, Mrs. Smith, who works from home using a computer shared by her teenager. If the teenager has spent much time at all using the computer, browsing social networking sites, communicating with the instant messenger, or and downloading software, then there's a good chance the computer is infected. And those infections can now affect your business.

Some viruses that attempt to propagate through your network gathering private information, deleting files, and launching attacks against other networks. Key logging software may capture Mrs. Smith's login information to allow unauthorized users to access the info later. Screen capturing programs may be reading private data as Mrs. Smith examines it on her screen. Trojan virus programs may be installed in your network to allow remote access to unauthorized users from other countries. These are just a few of the problems that can happen when malicious software invades a remote machine.

Yet telecommuting has many benefits and is encouraged, as long as the organization is protected. "The keys," says Foster, "are to have a healthy awareness of the dangers, educate your employees, and implement the latest security measures to keep your network safe."

Safety Precautions for Remote Workers

Foster offers the following suggestions for keeping remote workers from hurting your security.

- Some technologies can actually examine the remote computers before allowing a user to connect. If it doesn't meet minimum security standards, the connection can be refused.
- Other technologies can publish programs to the remote computer in such a way that the remote computer's interface is in a safety zone that's protected against most kinds of attacks.
- It's too much work for an IT professional to visit every remote computer on a weekly basis to check the security, so there are centrally managed solutions to automate this task. Your qualified IT professionals can help you identify the best solutions for your organization.

A common way to keep remote workers (and your network) safe are virtual private networks (VPNs), which enable remote computers to connect through the Internet as if they had a long network cable stretching all the way back to your office. This connection is helpful in connecting remote satellite offices as well as employees out in the field.

One advantage of having remote offices and employees connect to your main network is that it lets your IT professionals update and support remote machines automatically using the centrally managed tools in place at your main location.

"If one of your workers doesn't connect back to your main network often enough, he or she could be traveling on Patch Tuesday (the day Microsoft releases new patches) and not get a needed update until the next time

he or she is physically in your main office," explains Foster. "This could be a long time, depending on how extensively that person travels. That would make that computer vulnerable for an unnecessary period of time." It's best for patches to be applied within 48 hours of release.

You could mandate that everyone who is out in the field with a laptop must connect to the company's network every night, or at the very least, every three days. Some companies even give their employees wireless cards from companies such as Sprint or Verizon so they can be connected from virtually anywhere there is service. Then, as long as the laptop is connected, and the network is configured correctly, your IT team can run security updates, as well as anti-virus, anti-spyware, and personal firewall checks even on computers that aren't physically in the office.

According to Foster, this simple strategy will help prevent one of your employees from coming back to the office and bringing viruses and other malicious items into the company's network, because IT has a chance to regularly update, monitor, and service the machine. Best of all, the cost is very inexpensive and often based on the number of users connecting remotely.

Using a VPN has an additional security benefit: It provides encryption to the data being transmitted. Why is this important? So that attackers cannot easily capture and read the data in transit. Yes, it's possible for an attacker to read the data while it's being transmitted. For example, they could perform what is known as a "person in the middle" attack, but having a VPN makes the process more difficult.

With a "person in the middle attack," your remote user computers believe they are connected directly to the systems they are accessing, but in reality the remote computes are connected to an attacker's machine. The attacker's machine then connects to the main network system — hence the term "person in the middle."

"Realize that the hacker watches everything … credit card numbers, passwords, logins … *everything*," says Foster. "That's why you will benefit from using some form of encryption on your data when you connect to any of those networks in a hotel, coffee shop, or anywhere else. A VPN is one way to provide this encryption. This is just another reason to seriously consider security measures for remote connections to your company."

For remote users, the process of connecting to the office sometimes consists of two steps. First, connect to the Internet. Next, establish the connection to the office through the Internet. Your IT professionals may be able to make this a single-step process, and users at remote offices often have a VPN connection that is operating 100 percent of the time so there are no additional connection steps necessary.

What about Non-Company Devices?

These days, many employees are engaging in BYOD ("bring your own device"), where they use their own smartphones, tablets, and even laptops in the office to connect to the organization's network. Some employees will want to use these devices elsewhere too. At first, companies may think this is a great idea, because it saves them the trouble and expense of having to provide all those devices to their staff.

But as Foster warns, "Just because you trust the person is no reason to trust their device too. The device, especially laptops, may be infected without the user's knowledge — even if the user has their own anti-virus. Therefore, there are many steps to take to protect your network. For example, when that user uses a BYOD device to connect to your internal network, be sure they connect to a filtered subnet that is separate from your other internal subnets."

Foster advises that you treat these personally owned devices the same way you would treat a guest that visits your organization. Ensure all devices are isolated within their own area of your network, referred to as a subnet or subnets. Depending on discussions with your IT team, you may choose to provide the personal devices access to a connection that takes them directly to the Internet and prevents them from accessing your own network resources or subnets. In any case, no device should ever be connected to your network without

an IT professional's inspection and approval from executives who will be held accountable and who also fully understand the risks to your organization (and your customers).

You can use management software to control user devices. Make sure your workers all have passwords on their devices (a good idea anyway). You can enforce the ability to track the physical location of the device and erase (wipe) the device's memory if you suspect it may be lost or stolen. Management software can go to extremes, such as limiting the apps that can be installed, when and where the users can use their cameras, and the maximum number of email messages the device will be allowed to store.

However, be careful about implementing too many restrictions. It *is* the employee's device. If you need to provide heavy restrictions, you may want to provide the devices your employees use.

As time goes on, devices will increasingly have the ability to basically "be one device when connected to the company, with all restrictions in place" and "be the home device when not connected to the company, with no restrictions." In other words, the phone or tablet will work as two devices in one package.

Leaders at some organizations may decide to exit the whole BYOD methodology and issue new or sometimes refurbished devices for the users to use at work. This is one of those topics that will continue to evolve as more organizations implement policies about it.

Action Items

- If you have remote satellite offices that don't already have point-to-point or MPLS connections to your main office, and/or people who connect from off-site locations to your network, have discussions with your IT professionals about securing those connections through a VPN or some other type of encrypted connection.
- Ask if they know specific users who are exposing the network to unnecessary danger because of some condition on the remote user's computer.
- Talk with your IT team about BYOD policies and security options.

Expert Practices -- The Benefits and Risks of Cloud Computing

Most people have heard of the cloud by now. Yet executives still sometimes wonder, “What exactly does it mean to be computing in the cloud?” As Vistage speaker **Mike Foster** puts it, “While we techies have our own definitions for cloud computing, in its simplest form, any programs that are not installed on the local computer and any data not saved on the local computer can be considered ‘in the cloud’.”

With that said, Foster also notes that there’s a big difference between (1) storing information in the cloud, (2) using a program or application that runs in the cloud, and (3) going completely to workstation virtualization in the cloud. For example:

1. Storing information in the cloud could be via services like Microsoft OneDrive, Apple iCloud, Evernote, Dropbox, etc. Many executives use online backup such as Mozy, Carbonite, or CrashPlan.
2. You could use applications that run in the cloud, referred to as Web applications and SaaS (Software as a Service). Popular examples include CRM products such as Microsoft Dynamics Live and SalesForce. Google Docs and Microsoft 365 are other common examples. If you aren’t paying another company to host your Exchange, you might want to consider having it hosted elsewhere so you don’t have to deal with an Exchange server (especially if you have more than 50 email accounts).
3. Using hosted workstation virtualization may allow you to eliminate all servers from your organization. With this solution you pay a hosting provider a set fee per user each month. The provider then handles everything your servers used to do for you, and generally provides additional services that you may have deemed too expensive in the past — such as generator power, strict physical security with armed guards, and servers with automatic failover if one server dies. The upshot? You don’t ever have to worry about the servers again!

   In some models of hosted workstation virtualization (the ones Foster recommends), the provider even keeps all of your licensing, including Microsoft licenses, up to date for you. Imagine: No more worrying about buying licenses, no more servers, and no more needing server support! Your organization’s computers act as remote terminals, but they feel like powerful computers. Your users can be on a laptop, desktop, Mac, tablet, a device called a Thin Client, etc. — it won’t matter that much. Think of LogMeIn or GoToMyPC on a grand scale.

The main idea behind the second and third categories listed has two parts, explains Foster. “First, users can have icons on their desktop, click on an icon, and the user is able to work. Second, it is irrelevant to that user whether that program they launched is installed on their own PC, being pushed down to their PC from a server, running on a server on their corporate network, or being provided by a different company over the Internet. It is up to the IT professionals to handle the details — the users just have the information and tools they need to take care of your clients and their needs.”

There’s a good chance that your organization already uses a hybrid of these three categories — mixing cloud services with your existing technology — and that’s fine. You may move more to the cloud, or not. The most important part of using the cloud properly is to increase returns, reduce costs, and improve both your users’ and customers’ experiences.

Benefits of “In the Cloud” Computing

Foster offers the following list of benefits for using cloud computing.

- Many cloud services allow month-to-month contracts. This applies to storage in the cloud, using web applications, and even workstation virtualization.
- You don't need to install patches to the application — your cloud provider does that for you.
- If there's a disaster at your office, your workers can work from home or work on the road almost as easily as if they were at the office. This saves you a lot of time.
- Generally with cloud services, you and your users can access the cloud applications from practically anywhere using practically any device that has a browser — even a smartphone.
- You sometimes need less on-site support and/or may not need to hire more IT professionals in your organization. And, if you're already understaffed, your existing IT professionals will be able to focus on other important tasks and projects.
- Providers in the cloud often have highly trained and highly qualified professionals taking care of the network — professionals who would otherwise be very expensive for you to utilize their expertise.
- Backups are naturally off-site and are often more secure than your own backup solution. Most companies these days are very concerned about having a DRP (disaster recovery plan) in place, and utilizing the cloud can significantly enhance the ability to recover in the event of a disaster.
- Adding new offices, new users, and new applications is generally simplified due to instant scalability. This means your fees are adjusted accordingly and instantly as your number of users dynamically increases and decreases.
- Spam blocking, if you're using hosted email.
- If users are on the road and their personal laptop malfunctions, it's often less dangerous for the user to access via a "hotel business center computer" than if they used the hotel computer to connect directly to your internal network.
- You may not need a server room and, if office space is cramped, this can allow you to have more room for your office personnel.

Drawbacks of "In the Cloud" Computing

Of course, nothing in life is perfect, so Foster also offers the following list of drawbacks to cloud computing to be aware of.

- If your Internet connection fails, you can't use the services.
- If you have a slow Internet connection, your services may be slow, too.
- If the "cloud" company goes out of business, you may lose access to your data forever.
- Security concerns: Will the cloud company keep your data secure?
- In the past, it was easy to define the perimeter of your network as existing at your firewall. Everything outside your firewall is "out there" and everything inside your firewall is "in here." Utilizing cloud services for your private data blurs that line.
- The provider could accidentally delete your important data. This has happened before — even at some of the major cloud providers.
- Sometimes one of your organization's most important applications, such as your ERP, offers a cloud-based solution. If you have your internal application customized to populate forms in your word processing programs, etc., you may lose the ability to perform customizations if you move to the cloud.

- The same with sharing data between your local applications. Moving one of your most important applications to the cloud may eliminate the ability to share data with your other applications.
- It may be expensive to convert your systems to run in the cloud.
- Using a cloud service often adds one more entity to the finger pointing game of “the hardware guy blames the software guy, who blames the cloud provider, who blames the Internet Service Provider,” etc.

How to Use the Cloud Wisely

Many executives know to carefully examine their strategies. If you’re considering moving to the cloud, Foster suggests considering these important steps:

- Keep your own backups of all data in case the cloud provider ever loses it and can’t restore it.
- Establish your own business continuity plan (see “Your Disaster Recovery Plan”). This plan, which you may practice implementing one or more times a year, is what to do if your cloud provider fails.
- Have your legal advisor help you with your contract, making sure to includes clauses for both a service-level agreement and a quality of service. The former specifies how much of the time the provider will be up and running for you to use their services. The latter specifies how quickly the service will perform. You want a rapid response as opposed to applications that function so slowly that your user productivity suffers.

Whether to move some or all your services and applications to the cloud is a strategic decision. Foster reports that some companies are eager to move toward the cloud, while others are digging in their heels and refusing to make the switch. They do not want to trust the security of their private data to services, nor are they sure their data will be available when they need it. Still, some very large organizations are moving to the cloud and experiencing great results. The good news is that if handled correctly, the cloud can be very helpful for companies of any size.

Action Items

- Investigate the various cloud computing options that would make sense for your business.
- Weigh the pros and cons of moving to the cloud.
- Ask prospective providers what guarantees they will make you for their availability, called a SLA (service level agreement), and what their consequences are. If they tell you they’re allowed to have up to a 60-minute outage before it’s considered to be an “outage” for you, for example, and that they’re allowed to have up to 24 of those in a day, do the math. If their only consequence is to refund you one day’s worth of your subscription, that isn’t helpful when you’ve been “down” for a full day.
- If the pros outweigh the cons, make your move.

Tools & Analysis -- IT Security Assessment Form

Most CEOs are certainly interested in their company's security. That's why they install security systems in their office, keep valuable documents in a fireproof safe or at a secure, off-site location, and perform thorough background checks on all new hires.

But what about IT security? What about all that proprietary and confidential data stored on the company's computers? How safe is that? For most CEOs, the answer is "not very."

To assess where you stand in terms of data security, and to understand the risks to consider, ask yourself the following questions. (Please note that these questions don't cover every possible scenario, but will give you a good idea of how vital it is to follow IT best practices and take IT security seriously.)

1. How big a deal would it be if hackers managed to shut down your network for three days? For a week? For even longer?
2. Do you have any company secrets, such as your formula for doing business and/or pricing information, that you want to protect?
3. Have you, or has anyone you know, ever been affected by a data security breach of some kind?
4. Are you in complete compliance with the data security regulations that apply to your organization? Do you know which regulations apply to you?
5. When was the last time you audited your security? To ensure that you're receiving correct information, be sure the independent consultant has these three designations: CEH (Certified Ethical Hacker), CISA (Certified Information Systems Auditor), and CISSP (Certified Information Systems Security Professional).
6. When was the last time you talked with your IT support people, in-house or outsourced, about your data and network security exposure? Keep in mind that it's very difficult for them to be objective if you pay them for services. In other words, you'll get the most objective answers from an independent third party. Be sure that you provide them with a prioritized list of what you expect from them.
7. Does your organization have a strong password policy, or is the culture so relaxed that more than one person might know a specific password to a user's account?
8. If you carry a laptop with you, how secure are you when you connect at hotels and airports when you're traveling?
9. Finally — and this is a big one — have you discussed with your IT professionals how aggressive they are about applying your patches? Patches (fixes to security problems) need to be applied within 48 hours, but IT professionals need to hear that from you and you need to both provide some conditional leeway as well as set some boundaries for them.

Be honest with your answers. The more honest you are with yourself and your company's state of security, the better protected you can be in the future.

Tools & Analysis -- Checklist for Communicating with Your IT Team

It's important to realize that, of all the professional relationships that can make or break your business, your relationship with your IT support staff is among the most critical. In fact, it's just as critical as your relationship with your CPA, your banker, and even your attorney. When your IT staff feels supported and acknowledged, and when they're armed with the proper technology, they can single-handedly keep your company from losing data, losing work time, and losing customer confidence.

Since many of the suggestions in the **Vistage IT Security Best Practices Module** must be delegated to the IT team, many CEOs will benefit from knowing how to best communicate with their IT staff. Vistage speaker **Mike Foster** offers these quick guidelines to help make communications between the executives and the IT professionals more effective.

1. Ask for the bottom-line information. Some IT professionals can't always put into words why new technology is needed, even though it's often very important. You need to help them focus on the bottom line benefit the new technology will give the company. If an IT professional shares features and technical details with you in order to justify the purchase of a new technology, what do you do as the CEO? Most likely, your eyes glaze over and your mind drifts to some other topic. Before long you're staring at your IT professional and you see his or her mouth moving, but you're not hearing a word.

When you're talking with your IT professional and she starts telling you about all of the features of a new item, ask her point blank, "What is the ultimate benefit of this technology for the company?" Get your IT professionals in the habit of thinking in this manner.

2. Provide communications training. If you feel some members of your IT staff aren't always comfortable expressing themselves, then send them to communications training.

3. When an IT staff member seems to be trying to impress you with big words and acronyms, explain that **patient explanations focusing on the bottom line result** is what will impress you. Some, not many, IT professionals will use the "snow them until they glaze over" approach in order to shorten communications. Sometimes the IT professional justifies this by thinking, "Finally, they'll leave me alone so I can get some work done. In the end, they'll benefit more from my having fixed the problem than they will benefit from talking to me."

4. Empower your IT professionals with some authority (but not too much). If an IT professional team member says, "I will fix your printer in a little while because the network server is about to crash," then the IT professional needs the authority to make that decision and statement without being reprimanded later. It's very important that they can tell users, "Go fill out a trouble ticket and I'll fix the problem soon. If you don't fill out a trouble ticket, then I can't help you."

That may sound harsh, but unreasonable demands on an IT professional's already busy time just adds stress. That stress can possibly turn into resentment and frustrating communications. Or, maybe they just work themselves so hard that they start making mistakes and/or experience problems with their families who never see them.

5. Never reward IT professionals when they solve an "emergency problem." Instead, use better communication and ask them, "What could you have done to prevent this?" This question causes them to shift

into a more strategic way of thinking rather than a “put out fires” mentality. You can reward them later, after a period in which there haven’t been any problems.

And remember to reward them. Many executives only think about their IT team when something is broken. That’s not fair. Communications with your IT staff will improve dramatically when they start thinking more strategically, and when you start recognizing their contribution to keeping everything up and running.

6. Send your IT professionals to project management training of some kind. Often, IT professionals have to manage multiple projects that are behind schedule and over budget, yet few have formal project management training. When people understand Gantt charts, PERT charts, and work breakdown structures, they can provide you with much better estimates about when a project will be finished. They’ll also be able to update you anytime you want with a new projected completion date. They’ll be better at setting the scope from the very beginning and asking for clarification, and asking for your approval if the scope creep will significantly delay the project.

7. When you hire IT professionals, consider people and communication skills as well as technical aptitude. If the person’s technical skills are lacking, but she has aptitude to learn more, you can send her to training for technical skills. But if her people skills or communication skills are lacking, she won’t change until she reaches a hurt level in her life that is so bad that she decides to change herself. Also, understand that some IT professionals have a personality of wanting to work with “things” rather than “people.” That may or may not fit the culture of your company and the job position they are filling. Just don’t try to force a round pin into a square hole.

8. Ask your IT professional how he or she “feels.” If you find that your IT professional is abrasive, and you want to stretch him into new areas of growth, try asking him how he “feels” about some specific issue you know is going on in your company. With some IT professionals, you may see a blank glazed over look. “Feel? What’s that?” they may think. If and when your IT professional discovers his own feelings, the next step is to ask, “How do you suppose Suzie might feel when you tell her ____?” If the problem is too large, you may want to help them find another job at another company. Compassion is in order since many people had something happen that was so painful in their earlier lives that they basically “turned off their feelings” in order to maintain a will to survive. Some IT professionals gravitate to the profession just to avoid needing to feel their feelings. But your compassion doesn’t necessarily need to go to the extent of allowing them to damage your business.

9. Good communication boils down to levels of trust. How trustworthy do you feel your IT team is? This varies in different facets of technology depending on training, experience, and ability to communicate openly. If you ever have a “gut feeling” that your IT professional isn’t being totally honest with you, consider that a serious indication that something is wrong. Your IT team members have their finger on the jugular vein of your company. If you don’t feel good about them, you may sense some issues that go beyond communication.

If you don’t trust your IT team to always behave in ways that support you and your company, if you feel that you may do or say something that will make them angry and they might hurt your system and/or quit their job, then you’re basically being held hostage. And you never want to be in that position. Some IT professionals (probably not yours, but just so you know) are so territorial that they want to keep knowledge in their own mind and not share it. If that is the case, you need to ask that IT professional to put together a DRP disaster recovery plan that includes how you will recover if that IT professional gets hit by a bus. Have a certified IT auditor (CISA) come in to analyze your system for best practices. If your IT professional is following best practices, it’s much easier for an IT company and/or a replacement IT professional to step in and take over after you fire the old IT professional who is holding you hostage.

Remember, as the CEO, it’s your job to initiate open dialogue with everyone on your team, including your IT team. If you don’t, you’ll end up in a situation where your IT professionals will believe they can’t come to you with issues that affect the company. They’ll think, “I can’t bring this up to the CEO. Sure, we need to fix the

anti-virus problem, but I'm not going to get approval for the $19-per-machine cost to upgrade." In this scenario, you'll never know where your company's weaknesses are until it's too late.

Tools & Analysis -- IT Security: Executive FAQs

When it comes to IT security and best practices, executives have numerous questions. Below, Vistage speaker **Mike Foster** answers the top questions executives routinely ask.

Question #1: I need to find a new IT professional. Other than the questions we ask all of our prospects, what are the most important things I should I look for related to IT?

Answer: First, although it isn't technical, look for "people skills." It's easier to train technical skills than it is to train people skills. People aren't usually interested in changing their people skills until they recognize the need. Allen Hauge, one of the key business leaders in the U.S., sent out a newsletter on April 28, 2014 quoting Reed Hastings, CEO of Netflix, who said: "Do not tolerate brilliant jerks. The cost to teamwork is too high."

Second, realize that project management is a key ability in which IT professionals aren't often proficient. Especially if they claim to have managed a lot of projects, ask them to describe a Gantt chart and Work Breakdown structure. (Refer to this blog post, and this one, for short and simple explanations of each.) If they can't answer, chances are their projects didn't finish on-time with the deliverables met. But this is a skill they can learn.

Third, ask them how they would react when you ask them to disable the firewall on your network and eliminate passwords. Of course you'd never ask them to do that, but don't let on. You want to see that they will follow your instructions, no matter what. You are in charge, not them. The answer you'd want to hear is, without them being shocked, "I'd advise you of the pros and cons and let you decide. I'll follow your direction and just make sure you know the consequences of your instructions."

Question #2: What's the biggest problem you see with how companies handle outsourced IT?

Answer: Paying outsourced IT firms by the hour is by far the biggest challenge. If you do that, then stop it. When you pay them by the hour, what are you incentivizing them to do? Take longer. They don't need to plan the most effective and efficient way to produce your results because they know "missing the target a few times and changing course later in the project" won't cost them any money — but it will certainly cost you.

They don't mind "learning on the job" because you're paying them to be educated while they sit there looking up answers on Google. I don't mind so much that they're researching answers on Google, but I don't want you paying them by the hour while they do so!

Tell them you want a service for a "flat fee," and that nothing else will do. If they won't quote you a flat fee, they don't feel comfortable being able to know how long something will take. Perhaps this is "new territory" for them and they plan to figure things out as they go along. Or maybe they don't understand exactly what you want so they plan to "wing it" as they go along — since you're paying them by the hour to do so. Find more information about this topic here.

Question #3: What if my IT professional or IT Company wants me to stay on an older version of, for example, Microsoft Office or Microsoft Windows?

Answer: While being on the "bleeding edge" is no fun, using the newest products is usually a much better idea. First, why should you spend new money on buying old stuff? Second, about the only reason to wait is the learning curve for your workers to understand the new version. Fortunately, vendors such as Microsoft are

figuring that out. For example, when Windows 8 was released, a lot of companies resisted the upgrade because the user interface was so drastically different. Eventually, Microsoft figured out that the new interface was "costing them sales," so Microsoft provided ways for Windows 8 to seem like Windows 7. That's good because the newer version is faster, more secure, and provides many enhancements. It's okay to "wait a while to upgrade" so other companies can see if there are any problems, but waiting more than six months is likely going to hurt you more than help. And that wait time is getting shorter all the time.

Question #4: When my IT professional fixes a problem, should I applaud them?

Answer: Absolutely not. You should ask, "What could you have done ahead of time to prevent this from ever having happened?" By asking this, you're putting them more into a proactive thought process, which is very different from what they are likely used to: putting out fires. When you find your network becoming more stable than ever, with no fires to put out in the first place — that's when you applaud them.

Question #5: Mike, when you go into companies, how many of them have enormous problems versus those who have a few things wrong?

Answer: About 99 percent of them have huge security problems, and closer to 70 percent of them are wasting money or not using products that are the right fit. We do NOT ever direct people to specific brands; we are brand agnostic and encourage you to use brands with which your IT professional are already familiar and like. The problem is, even with the best IT pros in the world, some of them "walked into a nightmare situation" when you hired them. Not only have they not had a chance to fix the problems that existed before their arrival, but they haven't even had time to find all of the problems.

Additionally, realize that you wouldn't want a brain surgeon doing heart surgery, or a heart surgeon doing brain surgery. Both are very smart people, but each has their field of expertise. IT is the same way. Your IT pros are specialists in one or more areas, but there's always room for improvement in your network (and frequently, *big* areas for big improvements). A qualified third party can help you identify and remediate issues so you can save money and get more done. Be sure to pay a "flat fee," not per hour, and explain to them that you need a partner, not a service provider.

Question #6: Which is better, Apple or Microsoft? We're talking actual computers — everyone knows iPads are way cool.

Answer: They are both awesome. Apple tends to attract "trendy" people and those who are creative. For example, some graphic designers refuse to use anything but Apple. Many executives use Apple computers at home, and more and more at work too. Microsoft definitely has the major presence in businesses today. Microsoft operating systems have a tremendously greater selection of tools that make it easier for IT pros to manage organizations with many computers on a network. A better-managed network means you'll have better results, save money, and increase security. In short, Apple is great for homes, executives, travelers, and small networks. There are many benefits to using Microsoft at the office.

Question #7: What should I do to secure my home computer?

Answer: It would be so nice to have a "silver bullet" that would protect you. Applying patches for the operating system (both Windows and Apple) and the application programs is essential. See this article for info on how to repel attacks, and this article for info on how to avoid getting hacked. It's crucial to change one of the biggest misconfigurations in history: Granting users control over their own computer by giving them "local administrator rights." When the users have so much control over their systems, more control than most users would ever need, hackers can have the same control when they trick a user. (See "IT May Have Your Users Misconfigured!") It would take a book to list all of the "must do" items to make your computer secure; you'll find a great deal of information at my company's blog.

Question #8: I heard someone talking about “hardening” their computer. What is that?

Answer: Hardening a computer means uninstalling all programs and features you never use. It also means changing your settings so that most programs and services don’t activate during startup. Rather, you start them if and when you need them. Hardening your computer makes it faster and more secure.

Question #9: Should our company fix everything possible and then, once things are fixed, invite in a specialist to review the system?

Answer: No way! You’ll end up buying the wrong stuff and wasting money doing things that don’t matter as much as other things that do. Be sure you get someone who works for a flat-fee for 12 months — no hourly charges. Then they can be with you, partnering with you, and providing you with direction while you make the changes. They can do something nobody else can.

Question #10: We’re going to find someone to help us with security. What certifications should they have?

Answer: IT security is such an important and broad field. You want someone who is certified in these three areas:

- CEH: Certified Ethical Hacker
- CISA: Certified Information Systems Auditor
- CISSP: Certified Information Systems Security Professional
- If you accept payment cards, be sure they also have PCI DSS experience.