VIRTUALIZATION
CLOUD
APPLICATION DEVELOPMENT
NETWORKING
STORAGE ARCHITECTURE
DATA CENTER MANAGEMENT
BI APPLICATIONS
DISASTER RECOVERY/COMPLIANCE
SECURITY

# *Best Practices: Laptop and Mobile Backups Today*

Laptop and mobile backup is an emerging area for data protection. Learn what technology is available today as well as advice about what should and should not be backed up.



TechTarget

# Laptop and Mobile Backup Picture Continues to Improve

A COUPLE YEARS ago, if you asked a few IT pros how they were backing up laptops, most if not all would flatly say "we're not." And they definitely weren't doing anything to protect information stored on smartphones. Things look a little different today, but make no mistake: laptop and mobile device backup is still an emerging practice. Ask the same question today, and the answers might be exactly the same.

The reason for this is twofold. Many IT teams have assumed that little data is stored on laptops and mobile devices that isn't stored elsewhere on the network (and thus backed up). Many organizations have policies in place which require laptop users to save any data they want backed up on network drives. This, of course, requires end-user participation... you know how that story ends.

The other reason lies with technology vendors: Until recently, there haven't been great options available to perform backups of these devices. The challenge in backing up laptops and mobile devices, of course, is that they aren't always connected to the corporate network. So, they must be backed up over the internet, or whenever they reconnect. Depending on how long passes between backups, this could leave a lot of data unprotected.

However, the technology used to perform laptop and mobile backups has changed a lot over the past couple years and organizations have a lot more options to choose from. There are a number of upstart companies offering endpoint backup point products today, and the major enterprise backup software vendors have options available as well. This Handbook offers information on what's available today for laptop and mobile backup, how vendors are addressing the challenges associated with backing up these devices, and how to choose a solution that is right for your organization's needs. ■

Andrew Burton

*Senior Site Editor, SearchDataBackup.com*

# Challenges and Solutions for BYOD Backup

**Protecting more data** that is scattered in more places than ever before is the biggest challenge to backup administrators today, according to IT executives at a data management symposium.

IT executives at the symposium, hosted by backup software vendor CommVault Systems Inc., discussed their policies for dealing with bring your own device (BYOD) and cloud backup—two trends that threaten IT's control over critical corporate data.

Several of the execs said they deal with BYOD challenges by supplying workers with endpoint devices such as smartphones and tablets so they can monitor data on the devices.

"One of our biggest challenges is to know where all the data is, and that it's in places where we want it," said Branndon Kelley, CIO at American Municipal Power Inc. (AMP) in Columbus, Ohio. "We're staying away from BYOD. We're saying, 'We don't want you to bring your own device, but we'll buy you whatever device you want,' and let people get comfortable. Or else we won't be able to retain talent, and our workplace is not going to be a place that invites people who want to stay."

Tracy Riggio, IT manager of Temple University Health System Inc. in

Philadelphia, said her hospital also provides devices for its users, who are mainly physicians.

"A lot of our physicians use iPads to connect to Epic [an electronic health record system], so they have it right with them," she said. "We've had doctors ask to buy their own, but we tell them, 'It's not going to work. You like your email? OK; use ours.'"

> ***"We're seeing iPads and iPhones, where in the past, it was all BlackBerrys."***
> ***—GAIL BYMUN,***
> *director of enterprise storage and data protection, Fiserv Inc.*

Gail Bymun, director of enterprise storage and data protection for Brookfield, Wis.-based financial services firm Fiserv Inc., said her company's security department mandates that all corporate data resides on Fiserv-owned hardware.

"Data is not allowed to go to a personal device," she said. "They are very strict on that. We're starting to branch out and support more devices. We're seeing iPads and iPhones, where in the past, it was all BlackBerrys. There was pushback from employees because of the slow adoption of some tools."

Other experts at the symposium emphasized the importance of strict control over devices for data security.

"People want to bring in their own devices, and they have zero concept about backup and recovery," independent backup consultant W. Curtis Preston said. "It's a mess."

## DEALING WITH CLOUD BACKUP CHALLENGES

The same can be said for people who set up their own cloud backup, another issue IT execs have to deal with. Cloud use is difficult to control because users can go to cloud providers and provision their own storage online with credit cards.

"I'm never going to give up the storage side to the cloud," said Ed Donakey, vice president of strategic relations for genealogy organization FamilySearch International. "The compute side makes sense for the cloud; that's commodity-based. But for backup and recovery, we'll continue to monitor that ourselves."

Riggio said regulations in health care make it important for Temple Health Systems to keep its data on its own disk and tape.

"We don't use the cloud yet," she said. "It's still a security issue. We're a highly regulated industry, and we're held responsible. Should that cloud infrastructure go away, it would be a problem."

## HYBRID AND CLOUD OPTIONS

For security, she said Temple Health encrypts all of its data. Primary data gets encrypted on EMC Corp.'s VMAX arrays and she uses CommVault Simpana to encrypt data that gets backed up to disk and then moved off to tape.

"If a tape gets lost, we don't know if there's patient data on there, so we have to report it," she said.

Fiserv's Bymun said there are "pockets" of people in her company who use the cloud. Fiserv is an umbrella group of smaller companies, and there are different approaches to the cloud.

"Some businesses have gone out to the cloud on their own because we could not react quickly enough [to their request for capacity]," she said. "Now we have a focus group working at providing cloud and hybrid solutions for end users."

AMP's Kelley said he is worried about legal ramifications of "Joe User" going out and provisioning his own cloud backup. "I can't imagine any CIO would say, 'That's a good idea.' I would say, 'No, I invested half a million dollars in this infrastructure, let's do it this way.'"

> ***"We lose flexibility once we go to the cloud."***
>
> ***—BRANNDON KELLEY,*** *CIO, American Municipal Power Inc.*

Kelley said APM has a tiered approach to the cloud. It keeps critical "heart and lungs" data in-house, but has moved some important applications such as email to the cloud. The utility company also uses the Oxygen Cloud Inc. for file sharing.

"Cloud is a big part of our strategy," he said, but some things must stay internal because "we lose flexibility once we go to the cloud."

Kelley attributes the rise of BYOD and the cloud in the enterprise to users demanding the same level of technology at work as they have in their personal lives.

"What we're dealing with is the first generation coming into the workforce that's grown up around IT and computers their whole lives," he said. "The Internet has been part of their lives since inception. When I got into IT 13 years ago, you used to go to work and the technology was better there. The Internet was faster; the computer was nicer; they had better printing.

"You go into work today, and there are environments still running [Windows] XP and old technology that barely works. You have this new workforce saying, 'You can just leave me at home and I can do a whole lot better.' As IT leaders, we have to take responsibility for that," he said. —*Dave Raffo*

# Laptop/Mobile Backups: Technology Advancing, Challenges Remain

LAPTOP AND mobile device backups are an emerging area of data protection. There are a number of challenges associated with backing up devices that are not always connected to an organization's network. And, in the past, many shops have put the responsibility to backup these devices in the hands of users. However, that's changing and many shops are taking a more active approach to laptop/mobile backups. In this Q&A, learn the state of laptop/mobile backups today, including the available options for backing up these devices, what's driving interest in the technology, and the convergence of laptop/mobile device backup with other technologies.

***What are the main challenges associated with backing up laptops and mobile devices?***

There are a number of different challenges associated with backing up laptops, but perhaps the biggest challenge is that of intermittent network connectivity. Remote backups cannot be performed unless a laptop has established connectivity to the backup target. This could be an enterprise backup server or a cloud backup system.

Another common challenge with laptop backups is bandwidth limitations.

Even though high-speed Internet connections have become the norm, some connections may prove to be inadequate for handling backups and whatever else the user happens to be working on at the moment. This is especially true for mobile users who travel a lot, as some hotels provide painfully slow Internet connections. Furthermore, some hotel firewalls are configured to block connections to corporate networks or to well-known cloud applications. Such blockages may sometimes make it impossible to perform a remote backup of a laptop.

***Laptops have obviously been around for a long time. What's driving the increased interest in data protection on endpoints today?***

Laptops and mobile devices have always been a thorn in the IT administrator's side. For decades administrators have experienced the pain and frustration that comes with data loss related to laptops. It wasn't that administrators did not want to back up laptops, it was that until relatively recently there just was not a good way to do it.

The recent interest in backing up laptops and mobile devices probably has to do primarily with the fact that there are now practical ways of performing those backups. Of course, compliance concerns and the fact that more users are working from mobile devices today than ever before is also bound to play a role in the increased emphasis on laptop backups. The fact that there have been some high-profile examples of data loss is almost certain to also be a factor.

***How are organizations addressing laptop and mobile backups today? And, what are the various tools/approaches available today for backing up laptops and mobile devices?***

The ways in which organizations are addressing laptop and mobile device backups today are incredibly diverse. Some organizations continue to either provide no backups for laptops, or ask users to perform their own backups of anything important.

Other organizations attempt to backup laptops using a method similar to the way that they back up on-premises servers. This usually means installing a backup agent onto the laptop so that backups can run whenever the laptop has connectivity.

Cloud backups are also a popular option. Those organizations that are performing cloud backups typically either perform backups to private clouds or subscribe to a backup as a service provider.

The ways in which these backups are created can be quite diverse. Many organizations have begun licensing laptop-specific backup products that are designed to perform CDP-style backups. This type of software keeps track of which storage blocks are modified and when.

Whenever the user establishes connectivity to the corporate network or cloud backup service, the backup software automatically begins uploading any changed blocks, as well as a record of when each block was modified (to facilitate

point-in-time restoration). Typically, this approach uses deduplication to avoid having to retransmit any block that is already stored on the backup target.

There are also organizations that rely on the use of custom scripts to perform backups. Often, these scripts are referenced within the Active Directory and automatically execute when the user logs on to the corporate network.

As for mobile devices, the most popular option to date has been the use of apps that back the devices up to the cloud. However, these apps are often device-specific (Windows iOS, Android, etc.), which means that organizations might have to use a different app for each class of mobile device.

***Can you outline some of the pros and cons of each approach?***

Obviously, there are pros and cons to each of the backup methods that have been discussed. The use of a cloud backup service, for example, tends to work really well but it can be expensive because most cloud backup providers charge based on the amount of data that has been uploaded.

The use of custom scripts and scheduled backups both work well under the right circumstances. The main drawback to these approaches is that there are never any guarantees of how long a user is going to be connected to the corporate network. There is a very good chance that a user may log off before a backup completes.

CDP products that are designed for laptops can often remedy this problem

because they are designed to stream data to the backup target any time the user is logged on. If a user disconnects then the software resumes the upload process the next time that a connection is available. Some organizations have begun using technologies such as Microsoft's DirectAccess to ensure that users are connected to the corporate network any time that they have Internet access. That allows the backup to run, even if the user isn't accessing any corporate resources.

***What about desktop virtualization? Do you see organizations using that to address the issue of unprotected data on laptops? Or is it too much of an expense/undertaking for most organizations?***

The fact that desktop virtualization can simplify the backup process is simply an add-on benefit. It isn't usually a compelling enough reason by itself to make an organization adopt the technology.

It is important to remember that desktop virtualization assumes that any time a user wants to access corporate resources, they log onto a virtual desktop. The problem with this assumption is that there are likely to be times when the user does not bother logging on and simply works locally. I have yet to see an organization provide mobile users with access to virtual desktops, but also perform laptop-specific backups. This means that data stored on the laptop's local hard drive may still be at risk in spite of the investment made in desktop virtualization.

***Are there specific issues that need to be considered for mobile devices such as tablets and smartphones? Or can you just rely on the same tools you use to backup laptops?***

Devices such as tablets and smartphones normally provide a completely different set of challenges than backing up laptops. The biggest problem with tablets and smartphones is that, often times, they run a different operating system from what is running on laptops (with Windows 7 and Windows 8 tablets being the obvious exception).

Historically, a lot of organizations have completely neglected laptop and tablet backups. Until somewhat recently, there wasn't really any good backup software for them, and a lot of organizations assumed that not a lot of data was stored on these types of devices anyway. But some smartphones have as much as 64 GB of storage, thus making it possible to store large amounts of data.

Although backup software does exist for smartphones and tablets, a lot of organizations simply require users to keep all data stored on the corporate network rather than storing data on these types of devices. This makes the backup process a lot easier, reduces bandwidth charges, and eliminates the risk of data exposure in the event that the device is lost or stolen.

***I've noticed lately a lot of apps for personal use only offer iOS and Android support as RIM/BlackBerry devices continue lose***

***market share—is this the case with endpoint backup software as well?***
This is certainly an issue to some extent. There is no denying that BlackBerry and Windows devices have a smaller market share than iOS and Android. The bigger issue, however, is that it is difficult to find a backup application that works with multiple mobile platforms, and still does a decent job. A big part of the reason for this is that the mobile vendors build some serious limitations into the mobile devices, and these limitations severely impact the backup process.

To give you a more concrete example, Apple limits iOS devices so that only calendar data, photos, contacts, and videos can be backed up. Similarly, Android devices must be rooted in order to do a full backup. Otherwise, it is only possible to back up things like calendar data, text messages, contacts, call logs, system settings, and applications.

***Another trend we have been watching is the increasing convergence of laptop/mobile backup tools and collaboration/file-sharing tools. Is there a big demand for this in the market? And do you expect to see additional convergence with other tools/tasks?***
I think that, as time goes on, every enterprise backup application will eventually offer full support for backing up laptops and mobile devices. The vendors will be missing out on a huge revenue opportunity if they do not offer this capability. Never mind the fact that they will lose market share to competitors.

I also agree with the idea that collaboration and file share tools are beginning to blur together. However, I also think that there are some other areas to watch as well. I think that, as time goes on, we might see a convergence between backup software and image-based deployment software or possibly a convergence between backup software and virtual lab software.

Virtual lab software allows organizations to create a virtualized environment that they can use to test upgrades, new applications, patch management, etc. There are already some vendors that have begun experimenting with such convergences.

*—Brien M. Posey*

# Mobile Backup Issues and Options

USERS MAY BE carrying a significant amount of their company's intellectual property on their smartphones, tablets and other ultraportable devices—and that data needs to be protected.

First, a little math. Consider an organization with 5,000 employees, 20% of whom are knowledge-based workers with a reason to have corporate data on their mobile devices. Then assume that each worker is carrying 20 GB of corporate data on their devices. With a simple calculation, we can determine that this hypothetical organization has 20 TB of potentially unprotected data stored on mobile devices.

No organization would stand for a 20 TB hole in its data protection strategy inside its data center, yet such holes are routinely ignored outside the data center. Ironically, the data floating around outside the data center is at even greater risk for loss. It's easy to see how quickly small amounts of data across large numbers of devices can add up to a significant problem.

## WHAT'S A MOBILE DEVICE?

To start addressing the issue of data protection for mobile devices, let's determine

exactly what devices should be included under that term. Laptop PCs would represent the most significant repository of mobile data and, too often, they're overlooked as containers of valuable corporate data. Rapidly gaining ground as data repositories are tablets and sophisticated smartphones, which we'll refer to as "ultraportable devices." These devices have internal flash storage typically ranging from 8 GB to 64 GB, and many have secure digital (SD) card expansion slots, providing significantly more storage capacity. And you can expect the capacities of these ultraportable devices will continue to expand dramatically.

Organizations must recognize the potential risk these devices represent. Most have well-defined policies that prohibit the use of corporate devices for personal tasks. But this line is routinely crossed, whether the nonconforming activity involves personal email, calls, text messages, or document creation or editing.

Ultraportable devices make enforcing the line between personal and business use even more difficult. Users are increasingly employing personal devices they've purchased themselves for business-related activities and personal tasks. Examples include iPhones, BlackBerrys and Android-based smartphones that people use to connect to their business email accounts. iPads and other tablets may also be used to view, send and receive business email using Web browsers, and may be used to edit and store documents. Sales reps may be able to download price lists, proposal materials and other sales documentation using any Web-enabled device. It's becoming increasingly impossible and impractical to prohibit the mingling of

personal and business use of ultraportable devices. In many cases, it's a company's executives driving the move to allow tablets to access corporate resources. And if it's OK for the boss, others won't be far behind.

It's not unusual for a knowledge-based worker to have a laptop, tablet and a smartphone. Thus, in our earlier fictitious company example, 1,000 knowledge workers might be toting around as many as 3,000 devices, all with corporate data stored on them. To deploy a backup solution for this scenario you must address a high volume of devices with low volumes of data per device. Bandwidth is rarely a problem, but deployment, standardization, support and updates make it a challenge.

The deployment of ultraportable devices is growing exponentially, so the question is, how can IT managers get out in front and address the issue proactively? The good news is that it may be easier than you might think. The bad news is that it may be more complicated than some think it will be. Let's dissect the issues and see why this is a good news/bad news issue.

## YOUR POLICIES MAY NOT BE ENOUGH

Although organizations generally have clear policies regarding the separation of private and business use of devices, they rarely specify data protection requirements or procedures. Mobile device backup often falls between the cracks. Backup

is the domain of the data storage organization, but PCs are the domain of the end-user computing group, and cell phones are typically within the domain of the telephony or telecomm group. Tablets haven't found a place in most companies yet, so they may just be the domain of the user. So, the physical asset is managed by one group and the process by another; neither group assumes ownership. Hence, the first step in establishing a policy is determining who owns the whole operation. In practice, it will require the coordination of all groups.

***Tablets haven't found a place in most companies yet, so they may just be the domain of the user.***

This cross-functional complication is an excellent reason to consider outsourcing the whole thing to a cloud backup provider. Third-party providers will manage the whole process, including deployment, management and technical support. There may be cases, however, due to security, compliance (or corporate governance) or IT's reluctance to use third-party services, that make outsourcing an unattractive alternative. In those situations, IT must instigate the data protection policy based on business requirements.

Backup policies are ordinarily driven by recovery time objectives (RTOs) and recovery point objectives (RPOs). Mobile backup is a bit different and needn't be as complicated. RPO may not be easy to establish, as it may be driven by network connectivity, a daily backup schedule or product options. The variables of

ultraportable device availability make backup timing less certain than an always-on storage array in the data center. Information changes on individual devices aren't as volatile as data center devices. Therefore, recovery certainty is more important than backup timing. Moreover, a 24-hour RPO is probably a vast improvement over the intermittent or non-existent data protection users have today.

The essence of a mobile backup policy is pretty simple: who, what, when and how. The "who" can be the user (i.e., user-initiated backups) or system/software control (i.e., pre-scheduled and automatically launched). The "what" is the device, the "when" the backup event and the "how" the backup utility. That's about as complicated as it needs to get for typical applications and users.

## PC: THE CENTER OF THE MOBILE UNIVERSE

To get a handle on ultraportable devices, the first thing to do is to designate the PC as the center of the mobile universe. Some might argue that tablets are quickly supplanting PCs as a primary device. This may be true for certain tasks, such as Web surfing, video conferencing and even document lookup, but tablets still have a long way to go for effective document, spreadsheet or presentation creation. Tablets may be great display devices, but PCs remain the go-to platform for document creation. (This article is being written on a PC, while an adjacent iPad plays tunes.) Nobody does any serious document creation on a smartphone

and the inherent form factor of those devices makes it forever unlikely. The larger size of tablets may allow them to evolve to supplant PC functionality, but for the foreseeable future, consider PCs the hub of the mobile world.

From an ultraportable perspective, PCs play a key role as the central repository for syncing data with multiple devices. This will most often include calendars, contacts, email and the like. Yes, this data can and often is synced to external servers. However, BlackBerrys may be synced to a BlackBerry server, Exchange to an Exchange server and so on. By using the PC as a central syncing device, the user has one central location to recover data on a self-service basis. The added inherent remote sync gives the best of both worlds with user self-service and protection from data loss. Moreover, if one service experiences an outage, users have a "high-availability" solution from other devices. Not bad for what's essentially a no-cost solution.

*Organizations that don't have an automated laptop backup solution must seriously consider one.*

Placing the PC in this key role exposes the vulnerability of most PC backup strategies or, more accurately, the lack of a strategy. Even though they're well understood, they're not necessarily well protected. Organizations that don't have an automated laptop backup solution must seriously consider one. Convenient in-house solutions are available from most name-brand backup vendors, including

CommVault Systems Inc., EMC Corp. and Symantec Corp., and specialized vendors such as Druva Inc. Remote laptop backup is also a perfect application for the cloud, as provided by well-known vendors such as Asigra Inc., Barracuda Networks Inc., Carbonite Inc., Mozy Corp. (EMC) and Symantec's Norton products. Cloud-based solutions provide consistent policies across the organization, while minimizing the impact on the IT organization.

By using the PC as the central syncing platform, it becomes the backup server for the ultraportable devices. In most cases, the sync process is automatic. In this architecture, backing up tablets and smartphones takes less effort to protect corporate soft assets than one might think.

## DEVICE-SPECIFIC ULTRAPORTABLE BACKUP

Even though a PC-centric approach will protect the majority of corporate data, the plethora of applications for smartphones and tablets ensures that at least some users will continually push the devices into uses that no one could reasonably anticipate. Consequently, IT organizations shouldn't overlook the need to back-up the devices in addition to syncing them.

Let's start with the easy part of backing up smartphones and tablets. For those devices that use an SD card, or other such storage format, users can remove the card and copy it to a PC. Of course, this requires user discipline to do so on a

periodic basis. Periodic reminders from the help desk may be enough to foster the desired behavior.

The first thing one will notice when considering ultraportable backup is the fragmented nature of the task. Pictures, videos and music may be backed up to iTunes, Google Inc. Picasa or a PC. Application backup may go to Titanium Backup (Android) or the Apple Inc. Store. When looking into the specifics of these backup applications, one finds that they tend to be very use-case specific. Some may backup the Android home screen, for example, while others sync contact and calendar information, and still others backup files. Users who are serious about data protection may be forced to use a suite of applications.

This fragmentation obviously makes backup of ultraportable devices more complicated. Even so, it can be beneficial because IT organizations can tailor solution specifications for corporate data only. User data, such as pictures, music and videos, should rightly be the responsibility of the user. However, a corporate decision to deploy a particular encryption product may interfere with user data if it encrypts the entire device. This may lead users to disable the product, thus defeating the efforts of the IT department.

The next thing one will notice when searching for ultraportable backup is a shortage of name-brand solutions. Given the tens of millions of ultraportable devices sold, it would seem to have significant market potential. Symantec offers a free Symantec Mobile Management (SMM) Agent app in the Apple App Store.

The SMM Agent app requires an SMM enterprise server. Of the other 55 applications for "data backup" in the App Store, all are consumer-cloud or boutique-type solutions that don't appear to be geared toward enterprise deployment.

As IT organizations decide how to cope with corporate data on ultraportable devices, there are many factors to weigh. The first is how to cope with very large device populations, unpredictable connectivity and highly individualized environments. Despite these difficulties, best-practice organizations will address the need to protect corporate assets. Cloud-based solutions offer the advantages of offloading the deployment, management and support to specialists. Cloud providers will also be prepared to address the needs of enterprises.

For organizations that prefer to architect and manage their own solution, they must first decide which part of the IT organization will own and manage the solution. In deciding what tools to use, they'll find that ultramobile backup becomes a stack of its own. By focusing on what data is valuable to the organization, much of the peripheral personal data can be ignored. The task is to reduce the number of variables to those that count and thus make enterprise deployment a manageable process. —*Phil Goodwin*

AUTHOR BIOS



**DAVE RAFFO** *is senior news director with TechTarget's Storage Media Group. He joined TechTarget in 2007 after spending three and a half years covering storage for* Byte *and* Switch. *He also worked as managing editor of* EdTech Magazine, *as features and new products editor at* Windows Magazine, *and technology editor at eLearning company WatchIT. He previously served as an editor and reporter with United Press International in New York and a freelance writer for* USA Today, *Dow Jones and other publications.*

**BRIEN M. POSEY** *MCSE, has received Microsoft's MVP award for Exchange Server, Windows Server and Internet Information Server. Posey has served as CIO for a nationwide chain of hospitals and has been responsible for the department of information management at Fort Knox. You can visit his website at www.brienposey.com.*

**PHIL GOODWIN** *is a storage consultant and freelance writer.*

TechTarget

*Best Practices:*
*Laptop and Mobile Backups Today*
is a SearchDataBackup.com e-publication.

**Rich Castagna** | *Editorial Director*

**Andrew Burton** | *Senior Site Editor*

**Ed Hannan** | *Managing Editor*

**John Hilliard** | *Associate Site Editor*

**Todd Erickson** | *Features Writer*

**Linda Koury** | *Director of Online Design*

**Neva Maniscalco** | *Graphic Designer*

**Jillian Coffin** | *Publisher*
email@techtarget.com

**TechTarget**
275 Grove Street, Newton, MA 02466
www.techtarget.com



**About TechTarget:** TechTarget publishes media for information technology professionals. More than 100 focused websites enable quick access to a deep store of news, advice and analysis about the technologies, products and processes crucial to your job. Our live and virtual events give you direct access to independent expert commentary and advice. At IT Knowledge Exchange, our social community, you can get advice and share solutions with peers and experts.