Keeping an eye on IT essentials. ®

WHITE PAPER

Using Cloud Services to Protect Data Integrity with the Rise of User Mobility

This white paper discusses the challenges facing IT as the number of mobile users' increases and how Eyonic Systems' online backup service addresses these issues to provide data confidentiality, integrity and availability.

Table of Contents

Introduction

Maintaining business continuity at a time when users and their data are taking new and unknown roads is challenging. The increase of user mobility creates additional opportunities for data loss and file corruption, while also increasing business exposure. As a result, working to provide a stable and secure IT infrastructure is more complex than ever.

Threats against business data exist because private information is valuable. Keeping customer information private is valuable to both the company and the individual, and intact company files are integral to daily operations. For outsiders, gaining unauthorized access to business files provides a way to control the data which is costly to the business and those individuals whose information was captured.

Whether running a small business or managing an enterprise data center, data confidentiality, integrity, and availability are critical for business continuity. Cloud services provide an offsite disaster recovery copy of data while also protecting files from data sprawl and internal misuse. Maintaining an offsite copy of business data is an important step towards disaster recovery preparedness.

Recent Trends Increase the Risks Facing IT

A major game changer facing IT professionals today is the increase in the number of mobile workers. Supporting mobile workers requires much consideration to provide access to those who need it to do their jobs and keep everyone else out. In a study conducted by IDC, it was estimated there would be 212.1 million mobile workers in the US, Canada, and Latin America alone by 2015.[1] This figure is up from 182.5 million in the same regions just five years earlier.[1] Mobile workers are more likely to store singular copies of files locally on their devices putting them at a much greater risk if the device is compromised, lost or stolen.

Once a business has information worth protecting, there will be other people who feel the information is also valuable. Business information is often viewed as worthy of any effort to gain unauthorized access. Unfortunately, people often develop threats at a pace businesses cannot keep up with. In response to new and cleverer attempts to gain access to their data, businesses need to implement controls and procedures to protect their data from compromise.

Data breaches cost businesses time and money to recover from and can be catastrophic. Consider Anthem who admitted hackers were able to breach a database containing as many as 80 million records; records of current and former patients as well as their own employees.[2] Anthem is currently facing 26 lawsuits stemming from this data breach alone.[3] A study by IBM and Ponemon Institute released this year found the average total cost of a single data breach rose 23 percent to $3.79 million or $154 per record.[4]

The increase in the number of mobile workers has led to new challenges facing IT professionals in their quest to protect business data including:

- Data Sprawl
- Increased Access to Business Files from Remote Locations
- Increased Use of Personal Devices for Business Use

Data Sprawl

Having data spread across multiple devices is referred to as data sprawl. Data sprawl is growing at a rapid rate as the traditional singular business computer is replaced with mobile devices. Mobile devices are becoming lighter and faster with increased battery life, and each year there are more manufacturers and types. As the choices and value of features continue to increase, it is no surprise why people find themselves with more devices than ever before. Forecasts by Strategy Analysts say the number of devices per person in 2020 will reach an average of 4.3.[5]

Data sprawl is important to address because business information is important whether it is stored on a desktop computer, laptop, tablet or smartphone. Finding a way to protect business information on these additional devices becomes the responsibility of IT professionals. What makes this even more challenging is the fact that some of these mobile devices are never used at corporate locations. Luckily, cloud services are active once a device accesses the Internet and can backup company information without a device being located on the company network.

Increased Access to Business Files from Remote Locations

Greater than 75% of employees working from home do not use privacy guards when working remotely in a public place.[6] This means three out of four employees are not considering the security of business files when working in a public place by blocking strangers from viewing corporate information or accounts. While there are different types of data loss, each can be costly to a business.

Some examples are:

- Compromised data – when a device and/or files are infected with malware, viruses or spyware
- Physical loss – when a device housing unique data is physically lost, stolen or malfunctions
- Leaked data – when an unauthorized user gains access to data

In addition to information being exposed to strangers, people working in public places often use unsecured and unencrypted free wireless. Free wireless networks are susceptible to packet sniffing. Packet sniffing is a means of capturing the data packets a user sends from their device to the Internet and making a copy before it gets to its intended destination. Using this technique, it is possible to capture user ID's and passwords, copies of files, or emails with proprietary information.

Cloud services cannot prevent users from making bad choices when accessing business files. However, what they can do is ensure an uncompromised backup copy of business files exists, including previous versions, at an offsite and secure location. Cloud services also provide anytime access to files via the web interface so users never experience down time.

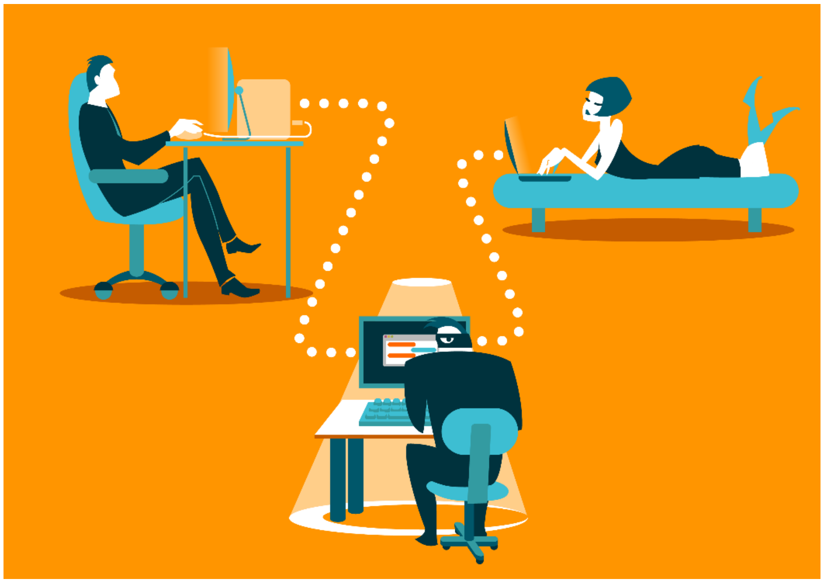


Image showing a man-in-the middle attack. Packet sniffing is a form of man-in-the-middle attack where a user sends information which is intercepted before reaching its intended destination. The information being sent may or may not be modified before reaching its intended destination.

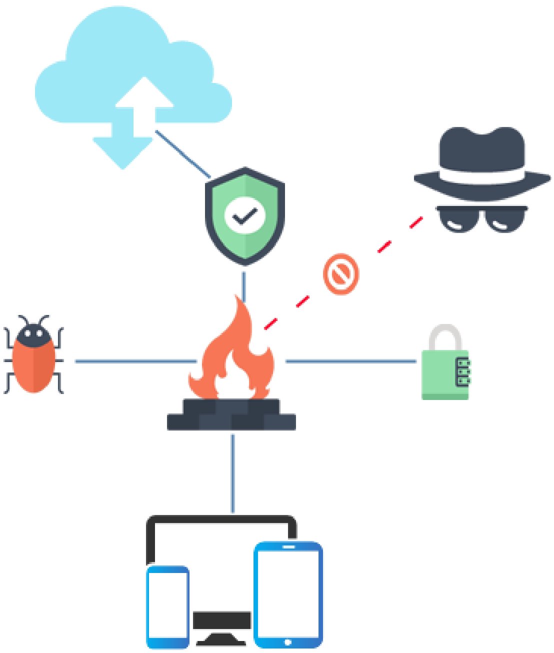
Increased Use of Personal Devices to Access Business Files

Another huge hurdle facing IT professionals is allowing remote access to users who need it while blocking access to everyone else. Even businesses who provide devices to employees with protective controls in place enjoy little guarantee for data safety. People often use their own personal devices which undoubtedly have lesser controls and protections in place. Unless a business configures their network to allow only those devices configured for each user, there is no guarantee the supplied device will be used by people connecting remotely to access business files.

The differences between using a business supplied device and a personal device can be huge. Most businesses typically employ the following to protect user devices and business files:

- Content filters – these block designated harmful and inappropriate content and file downloads.
- SPAM filters – these block harmful emails and remove harmful attachments from emails.
- Firewalls – these block attacks in many ways including blocking malformed packets, mitigating DDoS attacks, SQL injections, and disabling inactive ports that could otherwise be used to gain unauthorized entry into the network.

- Anti-virus and Anti-malware software – these run scheduled scans on user devices to detect and automatically remove infections without requiring user interaction. These can also run in real time to scan incoming and outgoing emails, provide safe web browsing, and scan files for malicious content before being accessed.



Personal devices are an increased risk to business data because they rarely have as many controls in place as devices managed by businesses. As the mobile workforce grows, this threat will rise proportionally. Already a massive 46% of remote workers admitted to transferring files between work and personal computers when working from home.[6] Moving business files between business and personal devices poses a serious threat to the integrity of business data. One benefit of using a cloud service for file backups is the ability to recover a file by rolling it back to a previous uncompromised version.

Challenges with Existing Backup Solutions

The two main types of business backups are:

- Traditional Onsite Backups
- Cloud Based Backups

Traditional Onsite Backups

Traditional backups include data backups created and stored locally. These backups can include tape backups, NAS devices, or other local storage. Storing a rotating version of recent backups at an offsite location is important when using a traditional backup solution. However, even when accompanied with offsite storage, access to the files is not available remotely and onsite backups do not protect data from natural disasters, backup hardware or media failure, or theft.

Some of the benefits of a traditional onsite backup are:

- Equipment and Data are all Local – Complete control over backup equipment and each copy of business data are controlled by the business. This reduces the physical risks to the data including theft, loss, or unauthorized access.
- Reduced Recovery Time – Traditional onsite backups are available for immediately starting the recovery process. Depending upon the connection type and network cards in place, communication between an onsite backup device and other equipment can be faster than downloading the data directly from the cloud. When recovering large amounts of data after an equipment disaster, this speed can prove extremely helpful in reducing costly down time.

Some of the limitations of a traditional onsite backup are:

- Backups only Capture Onsite Devices – Protections for user mobility are limited because mobile devices are often not used on corporate networks. This means files are one-offs stored on local devices which can put them at risk of being lost or compromised without the option to quickly and easily recover them.
- Lack of Offsite Copy of Data for Disaster Recovery – Traditional onsite backups are extremely limited in their ability to provide data recovery if at least one copy of the data is not regularly rotated to an offsite location. Often the backups are stored onsite causing them to have almost the same risk as the live files. If an offsite location is used, it needs to be secure and far enough away to avoid the same natural disasters. Offsite locations often add to the total cost of data backups.

Cloud Based File Storage

Cloud based backups use different procedures to protect files. By default, files using cloud based backup services are available at any time as they are hosted in the cloud. Any device with Internet access can recover files at any time using a web interface.

Some of the benefits of cloud based file storage are:

- User Mobility – Files on mobile devices can be backed up at any time as long as Internet access is available. Where and when a user connects from does not affect cloud based storage.
- Disaster Recovery – Files are stored at an offsite location meaning they are still accessible and recoverable in the face of equipment failure, theft or loss, vandalism, or natural disasters.

Some of the limitations of cloud based file storage are:

- Network Bandwidth Needed for Backups to Run – Initial file uploads, especially when large amounts of data are being transferred, can take days to run. This means business data could be potentially unprotected during this time until the first copy of the data is uploaded to the cloud account. As the initial upload runs, network bandwidth can become heavy and affect other programs using the network to communicate between devices and users.

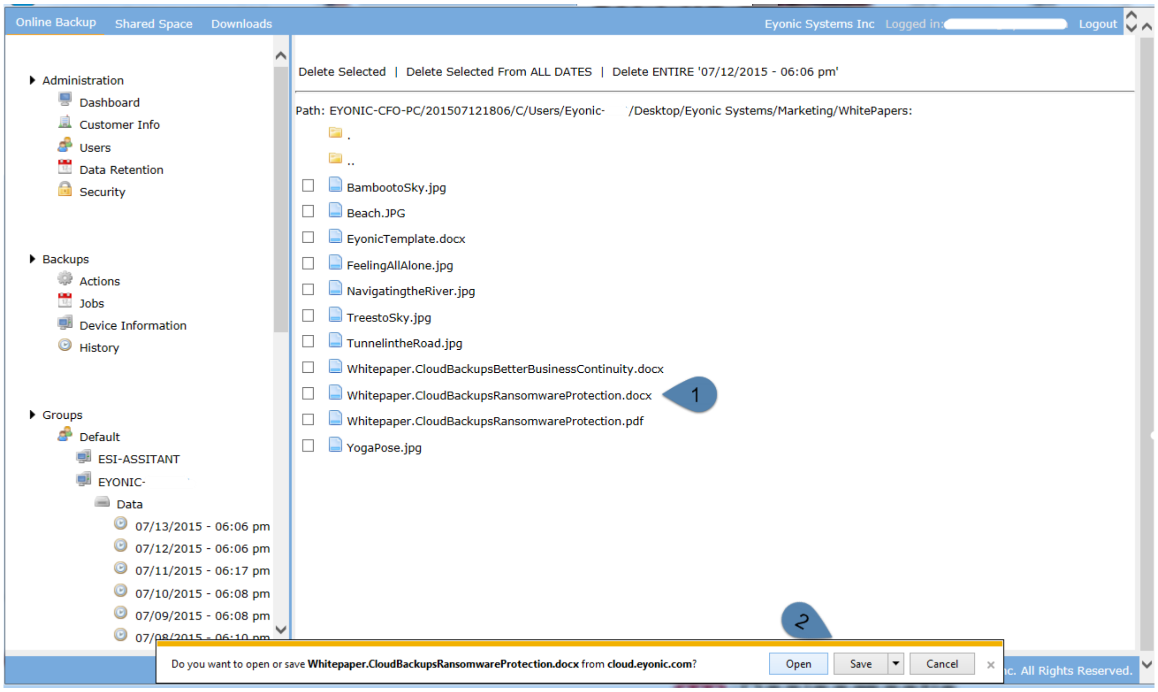
- Multiple Accounts – Multiple mobile devices may connect to different applications to back up their files. Having multiple data storage accounts to manage may not necessarily help reduce the effects of data sprawl.

Eyonic Systems' Online Backup Service

Eyonic Systems' online backup service is a cloud based service. With an offsite copy, business data is safe even in the face of natural disasters, onsite device failures, theft and loss. Our online backup service can save most businesses time and money as plans are scalable on demand. No need to sign up for plans based on future needs the way equipment must be purchased. Eyonic's cloud services allow you to sign up for current requirements and grow as needed.

Some of the other benefits of using Eyonic's online backup service are:

- Anytime Access to Files – Files can be accessed, recovered or downloaded from any device with Internet access at any time using the web interface. This means files are immediately available to a mobile user even if a device is lost or stolen. Simply log into the web interface from a different device and download or open files directly by navigating to the file and clicking, select open or save when prompted.

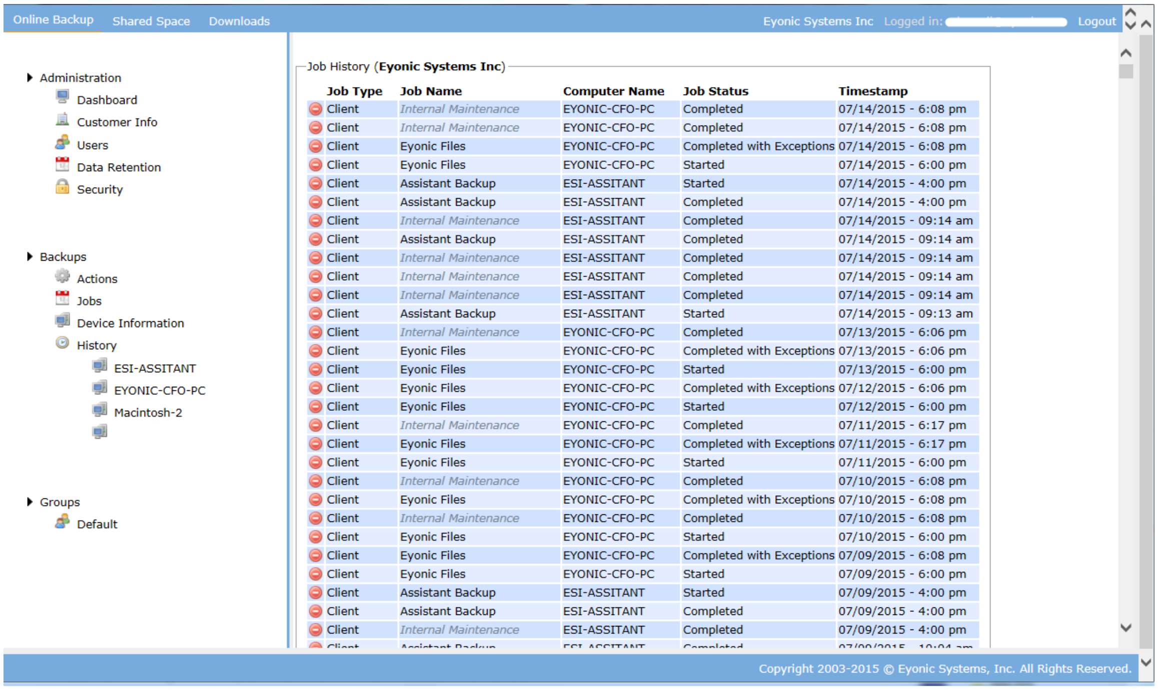


Path: EYONIC-CFO-PC/201507121806/C/Users/Eyonic- /Desktop/Eyonic Systems/Marketing/WhitePapers:

.
..
□ BambootoSky.jpg
□ Beach.JPG
□ EyonicTemplate.docx
□ FeelingAllAlone.jpg
□ NavigatingtheRiver.jpg
□ TreestoSky.jpg
□ TunnelintheRoad.jpg
□ Whitepaper.CloudBackupsBetterBusinessContinuity.docx
□ Whitepaper.CloudBackupsRansomwareProtection.docx
□ Whitepaper.CloudBackupsRansomwareProtection.pdf
□ YogaPose.jpg

Do you want to open or save **Whitepaper.CloudBackupsRansomwareProtection.docx** from **cloud.eyonic.com**?

- Mobile Device Files are Backed up Automatically – Scheduled jobs are automatic and run based on their scheduled time or as soon as they are connected to the Internet if a job is missed. Mobile users can be confident their files are being backed up even when they are working offsite because their jobs will run as soon as they connect to any network.
- Centralized Management for IT Professionals – Multiple devices can be added to a single Eyonic Systems online backup account. This is particularly handy because devices can be grouped together, group jobs can be applied to multiple devices, job histories can be verified for all devices or by a single device, and account storage is consolidated into one place.



Job History (**Eyonic Systems Inc**)

	Job Type	Job Name	Computer Name	Job Status	Timestamp
⊖	Client	*Internal Maintenance*	EYONIC-CFO-PC	Completed	07/14/2015 - 6:08 pm
⊖	Client	*Internal Maintenance*	EYONIC-CFO-PC	Completed	07/14/2015 - 6:08 pm
⊖	Client	Eyonic Files	EYONIC-CFO-PC	Completed with Exceptions	07/14/2015 - 6:08 pm
⊖	Client	Eyonic Files	EYONIC-CFO-PC	Started	07/14/2015 - 6:00 pm
⊖	Client	Assistant Backup	ESI-ASSITANT	Started	07/14/2015 - 4:00 pm
⊖	Client	Assistant Backup	ESI-ASSITANT	Completed	07/14/2015 - 4:00 pm
⊖	Client	*Internal Maintenance*	ESI-ASSITANT	Completed	07/14/2015 - 09:14 am
⊖	Client	Assistant Backup	ESI-ASSITANT	Completed	07/14/2015 - 09:14 am
⊖	Client	*Internal Maintenance*	ESI-ASSITANT	Completed	07/14/2015 - 09:14 am
⊖	Client	*Internal Maintenance*	ESI-ASSITANT	Completed	07/14/2015 - 09:14 am
⊖	Client	*Internal Maintenance*	ESI-ASSITANT	Completed	07/14/2015 - 09:14 am
⊖	Client	Assistant Backup	ESI-ASSITANT	Started	07/14/2015 - 09:13 am
⊖	Client	*Internal Maintenance*	EYONIC-CFO-PC	Completed	07/13/2015 - 6:06 pm
⊖	Client	Eyonic Files	EYONIC-CFO-PC	Completed with Exceptions	07/13/2015 - 6:06 pm
⊖	Client	Eyonic Files	EYONIC-CFO-PC	Started	07/13/2015 - 6:00 pm
⊖	Client	Eyonic Files	EYONIC-CFO-PC	Completed with Exceptions	07/12/2015 - 6:06 pm
⊖	Client	Eyonic Files	EYONIC-CFO-PC	Started	07/12/2015 - 6:00 pm
⊖	Client	*Internal Maintenance*	EYONIC-CFO-PC	Completed	07/11/2015 - 6:17 pm
⊖	Client	Eyonic Files	EYONIC-CFO-PC	Completed with Exceptions	07/11/2015 - 6:17 pm
⊖	Client	Eyonic Files	EYONIC-CFO-PC	Started	07/11/2015 - 6:00 pm
⊖	Client	*Internal Maintenance*	EYONIC-CFO-PC	Completed	07/10/2015 - 6:08 pm
⊖	Client	Eyonic Files	EYONIC-CFO-PC	Completed with Exceptions	07/10/2015 - 6:08 pm
⊖	Client	*Internal Maintenance*	EYONIC-CFO-PC	Completed	07/10/2015 - 6:08 pm
⊖	Client	Eyonic Files	EYONIC-CFO-PC	Started	07/10/2015 - 6:00 pm
⊖	Client	Eyonic Files	EYONIC-CFO-PC	Completed with Exceptions	07/09/2015 - 6:08 pm
⊖	Client	Eyonic Files	EYONIC-CFO-PC	Started	07/09/2015 - 6:00 pm
⊖	Client	Assistant Backup	ESI-ASSITANT	Started	07/09/2015 - 4:00 pm
⊖	Client	Assistant Backup	ESI-ASSITANT	Completed	07/09/2015 - 4:00 pm
⊖	Client	*Internal Maintenance*	ESI-ASSITANT	Completed	07/09/2015 - 4:00 pm
⊖	Client	Assistant Backup	ESI-ASSITANT	Completed	07/09/2015 - 10:04 am

- Backup Jobs are Quick & Bandwidth Efficient– All folders and files are scanned for changes before being uploaded allowing backups to be quick as only new and changed files are transferred to the cloud. Additionally, all data is deduplicated and compressed before sending, reducing the impact on bandwidth which is more important on mobile devices connecting to different networks.
- Endpoint Backup – With files on desktops and laptops being backed up, business information at any location is safeguarded. The ability to backup data anywhere it lives is a critical component of business efficiency and continuity.

Service Comparison

The following table breaks down the different features and their availability with each type of service including Eyonic Systems' online backup service.

	Traditional Backup	Cloud Based File Storage	Eyonic Online Backup
Offsite Location for Disaster Recovery	○ N/A	◐ Limited Capabilities	● Complete Backup
User Mobility	○	●	●
Anytime Access to Files	◐	●	●
Bandwidth Efficient for Mobile Devices	○	●	●
Centralized Management	◐	○	●
Endpoint Backup	○	◐	●
Automatic Backup for Mobile Devices	○	◐	●
Quick File Backups	●	◐	●

Conclusion

With the increase in user mobility, protecting all business data is a real challenge. Maintaining business continuity requires keeping the confidentiality, availability and integrity of data at all times. This includes company data regardless of where it is located, what device it is stored on, and who is accessing it. Protecting this data requires a balance of allowing access employees to be mobile to do their jobs and providing a backup solution to protect their files no matter what issues they run into. Recent trends including data sprawl require better disaster recovery protections if business data is going to stay safe. User mobility including accessing business files from remote locations have only proved to make it harder to maintain accessibility while preventing unauthorized access.

Eyonic Systems' online backup service provides data protection in multiple ways. With an offsite copy, business data is safe even in the face of natural disasters, onsite device failures, theft and loss. Backing up mobile devices reduces the problems associated with data sprawl and provides anytime access to files for users working away from the corporate network. Additionally, because files are scanned, deduplicated and compressed before being uploaded, backup jobs are bandwidth efficient for those mobile users.

Backup jobs run automatically based on a schedule so whenever mobile users connect to the Internet they are assured the same data protection as everyone else. Connecting multiple devices to a single account is storage efficient and consolidates business devices together. Lastly, centralized management provides an easy method for managing endpoint protection to meet the needs of your business every step of the way.

References

1. "Mobile Worker Population to Reach 1.3 Billion by 2015: IDC". *eWeek*. January 6, 2012.
2. "Millions of Anthem Customers Targeted in Cyberattack". *New York Times*. February 5, 2015.
3. "Anthem faces lawsuits over data breach". *FierceHealthPlayer.com*. July 13, 2015.
4. "Data breach costs now average $154 per record". *ComputerWorld.com*. May 27, 2015.
5. "Number of devices to hit 4.3 per person by 2020 – report". MoblieWorldLive.com. October 16, 2014.
6. "Data Leakage Worldwide: Common Risks and Mistakes Employees Make". *Cisco*. 2008

About Eyonic Systems

Eyonic Systems is dedicated to simplifying technology. We offer a suite of responsive technology services for people and businesses with any level of experience to save them time and money. These services include network integration, online backup, drive destruction, and enterprise file sharing. Our services are built to provide the confidentiality, integrity, and availability people expect from technology services. Our services are a great value because they are flexible and provide on demand scalability.

Businesses of all sizes and types use Eyonic's services to safely manage their offsite data both for disaster recovery and accessibility. Whether protecting data, sharing data, or preventing data from falling into the wrong hands, we have a service to meet your unique needs. We believe protecting the integrity of data starts with the right network design, and does not end until equipment once storing data is professional destroyed.

Eyonic is a privately held business located within the United States. For more information, visit us at www.eyonic.com. To get started with your free 15-day trial, visit www.eyonic.com/signup.

Connect with Us

1-855-439-6642
1-707-317-1167 Fax
607 Elmira Road Ste 113
Vacaville CA 95687