

Security vs. Disaster Recovery

Three Best Practices of Disaster Proof Hard Drive Technology

Robb Moore
CEO of ioSafe

Table of Contents

<i>Introduction:</i>	3
<i>Balancing Physical Security and Disaster Protection</i>	3
<i>Emerging Technology: Disaster Proof Hardware</i>	3
<i>The Big Picture: Data Loss Causes</i>	4
<i>Best Practice #1: Physical Security in the Data Center</i>	6
<i>Best Practice #2: Remote Office / Branch Office</i>	8
<i>Best Practice #3:</i>	
<i>Balanced Security and Disaster Recovery for the SMB</i>	9
<i>Conclusion</i>	11

**Introduction:
Balancing Physical Security and Disaster Protection**

In the world of product design, a common saying when considering a new product concept is “good, fast and cheap – pick two.” The majority of decisions are always a balance of high quality, features, time to market and cost of goods. Sacrifices are always made somewhere – you can’t have it all.

The Marketing Department can request a product that is ultra light weight, stronger than carbon graphite yet cost pennies per pound. Engineers love to specify “unobtainium” as the material of choice for such a challenging problem. Be advised though, availability is extremely limited.

In the world of data protection, similar balances exist when implementing a comprehensive plan. Security, disaster recovery, ease of use, compliance and cost are often considered and require a balanced approach for any size company. Balancing all the aspects of data storage will sometimes involve heated negotiations between company divisions.

The IT department wants a system that is easy to manage. The compliance officer won’t be satisfied until she can breeze through the audit. End users will demand ease of use. The CEO cares more about profits. If your “brilliant” security and disaster recovery plan sinks the company in the process, will the CEO approve it? Different company divisions will have conflicting goals and objectives – you can’t have it all.

Emerging Technology: Disaster Proof Hardware

Almost all data resides on hard drives. Hard drives are everywhere. The lowly hard drive does almost everything well. They are “good, fast and cheap” for almost all scenarios wherever data is stored. Standard hard drives have a big problem....they’re not disaster proof. Vulnerability to fires, floods and physical damage force anyone with a hard drive to consider contingency plans in case of disaster.

Balances exist when implementing a comprehensive plan.

Hard drives have a big problem... they’re not disaster proof.

**Firefighters
won't ask
your
permission
before hosing
down your
server.**

The natural disaster vulnerability of hard drives has shaped industries. Offsite vaulting and online backup exist to some degree to resolve this particular hard disk drive weakness. What if hard drives were not vulnerable to fire or water damage?

Would still pay a monthly fee for backup if your data was already flood proof? Would you risk dropping the tape or drive backup in the parking lot in order to protect the data against fire if your server was already fireproof? Would you still need pay for more bandwidth if you weren't trying to push a 2 TB backup through your T-1 line if you could bolt the 2 TB to the floor?

Encryption and network security are often used to protect data. Wildfires and hurricanes care little about whether the data is encrypted. Firefighters won't ask your permission before hosing down your server.

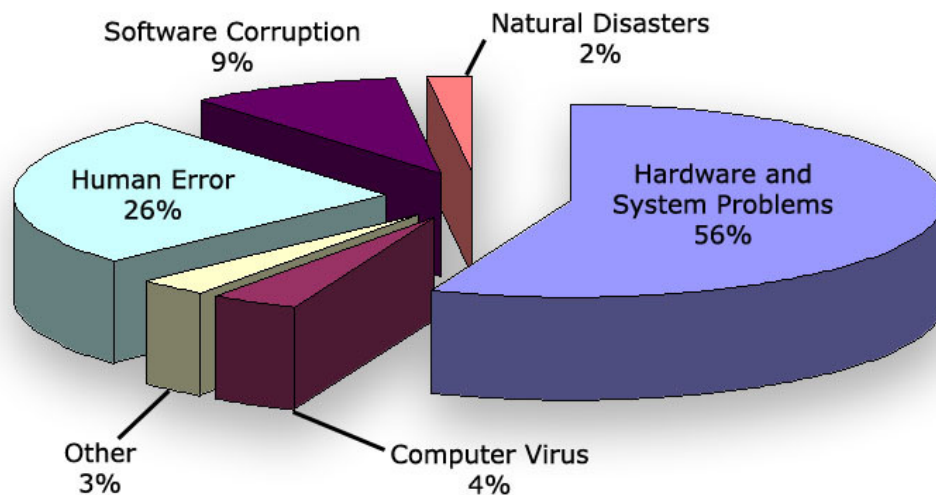
Physical security of data is often overlooked. Designed to be bolted to the floor or padlocked to anything immovable, the steel outer casings of disaster proof hardware combined with fire and flood protection are designed to provide the ultimate physical security for external data storage.

This whitepaper explores the proper application of fire proof & waterproof data storage hardware to add physical security and balance it with disaster recovery. Fireproof and waterproof hard drives can be used to improve data security and disaster recovery wherever vulnerable data resides. When considering disaster proof hardware technology, dramatic improvements in risk and security can be gained for very little comparable cost.

The Big Picture: Data Loss Causes

Data protection can be complicated. Every business has a different set of parameters by which the corporate culture and overall business objectives will dictate how "good, fast or cheap" solutions are balanced.

According to industry statistics, data loss can be attributed to multiple factors below:



Disaster proof hardware can be used to add security and disaster protection for very little cost or time impact.

Hardware, human error and software corruption account for the lion's share of data loss. Natural disaster, while a small sliver of potential causes, should never be overlooked due to the potential severity of the data loss. Up to 94% percent of business cannot survive catastrophic data loss. Protecting against natural disaster is often the most costly part of your protection budget.

The "big picture" doesn't just include disaster protection. Security and cost will also need to be considered in a holistic approach to balancing data protection objectives with business objectives.

Disaster proof hardware can be used to add security and disaster protection for very little cost or time impact. Due to the nature of disaster proof hardware, there is typically no extra maintenance or ongoing monthly fees when compared to non-disaster proof data storage devices. When used with existing technologies, disaster proof data storage technology can be combined with existing strategies in order to optimize value by balancing the most protection with each dollar spent. Amortized over the years, disaster proof technology can cost less than one cent per GB per month – a value that should not be ignored in today's economy.

Selecting the right location for your data center is paramount.

Best Practice #1: Physical Security in the Data Center

There are a number of resources that one can use to provide physical security in the data center environment. Selecting the right location for your data center is paramount. Putting your data center on the San Andreas Fault or in a flood plain is not a wise choice no matter what other physical security measures are employed. The best data centers use thick cement walls, have controlled access for cars and people as well as redundant technologies for power and internet connections.

The technology and strategies are well known and fine examples of data centers exist all over the world. Numerous documents available from the federal government as well as the National Fire Protection Association and telecommunications industry are available for reference.

The most expensive data centers are built at least in pairs separated by hundreds of miles. They employ high bandwidth redundant data lines to synchronize data and provide automatic failover. Pure synchronized data centers are of the highest cost and represent the best of class solution when price is no object.

In these economic times, being frugal is required for company survival. Significant cost savings can be gained by making the data centers asynchronous but a compromise must be made for disaster recovery. The lower costs of asynchronous backup will result in greater risk of loss during natural disasters. During a disaster, it will be possible to lose some finite amount of data. Data loss may occur if the data can't get out of the affected data center before the fire or flood. The application of disaster proof hardware to improve data security to reduce the data loss to zero and lower data center costs should be considered when architecting a system.

The emerging field of disaster proof storage hardware includes a handful of companies. ioSafe, Axxana, Sentry Products and FireKing offer a wide variety of options to consider.

In these economic times, being frugal is required for company survival.

**Lowered
monthly
connection
fees and
millions of
dollars can
be saved
with
relatively the
same net
effect of zero
data loss**

In the high end data storage environment, Axxana's Phoenix Enterprise Data Recorder (EDR) product is a fireproof, waterproof and crush proof solid state storage device designed to withstand all physical damage short of a direct nuclear blast. At over 400 lbs, it is inherently secure from theft as walking out the front door with it will not be a trivial task. It is expected to interface with a wide variety of enterprise class data center products and cost somewhere in the six figures. The return on investment (ROI) justification can easily be made in the dramatic savings when compared to the additional cost of a synchronous data center. Lowered monthly connection fees and millions of dollars can be saved with relatively the same net effect of zero data loss between data centers during disaster.

The downside of disaster proof technology includes the possible inability to retrieve the data in case of building quarantine. Axxana mitigates this objection by incorporating a cellular connection link to the data storage device. Recovery time to retrieve the data contained on a disaster proof device still may be a factor. A balance of speed vs. cost will need to be considered when comparing asynchronous centers vs. synchronous centers. The Axxana solution should be a strong contender when balancing the factors around data center deployments.

When considering mid or lower tier enterprise data storage, the ioSafe R4 Network Attached Storage / RAID system can also offer fire and water protection to physically secure vulnerable data. Weighing in at 120 lbs and storing up to 4 TBs of data, this NAS device is meant to provide a disaster proof backup target for any vulnerable data. This system can also be used to provide security to surveillance video or real-time natural disaster protection to data in between online backup or offsite tape vaulting events. Cost of the ioSafe R4 ranges from \$11K to \$16K.

For video surveillance, the ioSafe R4 is a great solution for securing and protecting video data that is typically never streamed offsite. In a casino, how valuable would the surveillance data be of cash left on the tables as people evacuate during a fire? The surveillance data could be the

difference between survival and death of a business when demonstrating the proof to your insurance company after the disaster.

***Best Practice #2: Remote Office / Branch Office
Achieving Balance outside the Data Center***

The Remote Office / Branch Office (or ROBO) data often sits outside the protection and security of the Data Center. In fact, by some estimates up to 70% of data resides outside the data center in stand alone computer systems and laptops.

ROBOs have the added disadvantage of no IT staff located onsite. DR, compliance and security are much more difficult to manage outside the controlled data center environment.

Backing up to tape and then transporting to an offsite location might be fast but often times it's neither good nor cheap. Lost tapes, unreliable recovery, managing encryption keys and vaulting fees are just some of the reasons tape is so unpopular for backup and disaster recovery. For archiving though, tapes might be a great solution. Don't forget to have a plan to migrate all the data to new formats before it's too late. I have a whole collection of personal Zip® disks that can be (easily?) read with my parallel port Zip® drive. It's possible now but wait ten years and ask me again.

There's no such thing as fool proof – when strategies evolve, natural selection theory kicks in to produce a more genetically enhanced fool. Transporting physical tapes or disks outside the company is decidedly not "fool proof". The news archives are loaded with stories of large enterprises and governments who have lost SSNs, credit card numbers and other critical data. Tapes are dropped in parking lots or lost in the mail. Humans in businesses large and small can hardly be counted on to reliably swap data storage from offsite locations. Is it wise to have a future disgruntled employee transporting the customer database to their homes? What happens to the data when this person is fired and starts working for the competition? While trying to protect against disaster, a company

Transporting physical tapes or disks outside the company is decidedly not "fool proof".

As long as the data amount is small...it's hard to beat online backup

Recovery speed is the key. Retrieving one file takes seconds. Retrieving one terabyte might take weeks online.

The most typical disaster recovery plan at the SMB is no plan at all.

exposes itself to daily security risk! Humans in the loop are almost never the reliable or secure way to go....certainly at times very foolish.

Online backup would seem to be the savior and sounds like it's solidly in the "good" camp. As long as the data amount is small and you're not interested in protecting the entire server from any disaster, it's hard to beat online backup for protecting small individual files from accidental deletion. Recovery speed is the key. Retrieving one file from online backup to recover from an accidental deletion might only take seconds. Retrieving one terabyte from a typical online backup site might take a few weeks. Uploading one terabyte might take months. Overnight delivery (aka the "sneaker-net") will be your best bet if recovering a large amount of data is required - hardly qualifying for "fast". One terabyte of business class, HIPAA or PCI compliant, 24/7 online backup won't qualify as "cheap" either. By itself, online backup is not a complete solution for any business with a server.

A recent deployment of disaster proof hardware to a large pharmacy chain demonstrates its versatility. By providing extra security, DR and HIPAA compliance aspects in one package, disaster proof hardware allows the distributed data in the pharmacy chain to be secure and compliant. Additionally, IT staff at the corporate office can remotely verify that backups are occurring without needing the help of the local store manager.

Best Practice #3: Balanced Security and Disaster Recovery for the SMB

The small/medium business (or SMB) is especially vulnerable to disasters. Over 98% of the 25 million businesses in the US have less than 100 employees. The SMBs are hardly setting up multi-million dollar data centers.

The most typical disaster recovery plan at the SMB is no plan at all. The second most popular is moving external hard drive offsite once a week - offsite vaulting. According to Murphy's Law, the server room will catch fire the morning before you are scheduled to take data home

with you. You will have not lost just any weeks data but it would be the most important – what you were just working on. Customer databases, accounting information and critical design data could all be lost.

Without professional business continuity and disaster recovery planning, the balance the cost of security vs. disaster recovery is more apparent for the SMB.

While offsite vaulting is popular in the SMB space, alternatives to this strategy include vaulting onsite using a safe with tapes or external hard drives. Be advised that there are two main kinds of safes: media safes (designed for floppy disks, tapes and CD's) and standard safes (designed for paper). Media safes are designed to stay at a lower temperature during extreme fire conditions. Any plastic or polymeric disk stored in a standard safe might not be as secure as you think. Temperatures up to 350°F inside a standard safe can be experienced in the worst of fires. This will surely melt CDs and tapes contained inside the safe.

The average fire lasts 15-20 minutes with temperatures of 800-1000°F at desktop height. Closer to the floor is cooler. Up at the ceiling can reach be as hot as 1400°F. A propane factory fire will obviously be hotter and burn longer than a sparsely filled factory floor. All fires need fuel and oxygen to burn. Once the fuel or oxygen is gone – the fire stops.

Typically fires in a small office building may result from the server power supply catching fire only to be extinguished by the automated sprinklers. Some SMBs store the backup tapes on top of the server – this of course would not be a good strategy.

Almost all fires have water present. In fact, a majority of the damage is not caused by the fire at all but by the water present from fire hoses or sprinklers. Be sure your safe or disaster proof hardware can protect against water damage as well as fire. If your media safe does not have provisions for water protection, use Ziploc poly bags to store your tapes and CD's when they're placed in the safe.

Disaster proof hardware offered from ioSafe, Sentry Safe or FireKing can mean the difference between survival and

The average fire lasts 15-20 minutes and is typically at 800-1000°F

Almost all fires have water present

Data storage requirements are compounding at over 100% per year.

death during a catastrophe. Starting at \$150 and storing up to 4 TBs of data, disaster proof hardware is designed to be simple to connect and protect data against physical threats in real time.

Since disaster proof hardware devices are hard drive based, one can image the entire server hard drive onto a disaster proof hard drive. Incremental, differential and continuous data protection software can be used with this hardware. If your internet connection is lost, you still maintain your ability to both backup and recover onsite!

For some businesses, it makes a lot of sense to transition every system and data storage as much to the "internet cloud" as practical. For the vast majority of businesses though, custom applications and exponential storage requirements could limit the businesses ability to store and operate purely in the cloud.

Data storage requirements are compounding at over 100% per year. Internet connection speeds are not compounding at an equivalent rate. The data will have to be stored and protected somewhere. Onsite storage in hard disks at the SMB location with cloud based remote access will be a popular choice.

Use of disaster proof hardware for the SMB does not impede the use of any other technology. The SMB can still use tape drives for archiving or continue to also use online backup for the most critical databases. For onsite recovery of the server in the fastest method possible, onsite external hard drives will be tough to beat when compared to tape or online.

To the SMB, speed of recovery can mean the difference between keeping a customer happy and having them go next door.

Conclusion

In the final analysis, spending money on disaster protection and security is like buying insurance for your data – the one thing that standard insurance can't get back for you once lost. If a business feels an impact of \$100K from certain data set that has a 1% chance of being lost, what is the appropriate budget to overcome

No amount of insurance can ever replace your data.

this possible loss? From this example, \$1000 is probably a good place to start. If you can come up with a way to spend less than this, you're getting a deal. Spend more and you're wasting money. Spending \$10K to cover a 1% chance of losing \$100K would be like risking a dollar to win 50 cents on the flip of a coin - not a good bet.

Business decisions can be complicated and you can only hope to have simple decisions like the example above. Credit card processing data centers have a different perspective on disaster recovery vs. security than small dry cleaning businesses.

At ioSafe, we use a combination of fireproof, waterproof external hard drives with disaster proof NAS/RAID storage and continuous data protection backup of the server's drives. Each night we trickle our small super critical databases online (encrypted) to guard against thermo nuclear war. Our email system is web based and accessible remotely but also replicated on our local systems. It's not perfect - nothing is. But for our SMB, this minimizes the human factor, protects from viruses and hard drive mechanical failure, maximizes security, gives real-time bare metal restore capability after fire or flood at a very low cost - not bad for a couple thousand dollars and no monthly fee!

Striking the right balance between security and disaster recovery is important in business of all sizes. Whether the data is at risk for a few seconds or weeks, protection and security can be added with almost no impact to the existing business processes while leveraging disaster proof hardware technology. Protection of vulnerable data wherever it resides, while providing a pragmatic, balanced approach to physical security is now possible - without an internet connection or human interaction.

Insurance can replace your office furniture, your servers and even your entire data center in the event of a disaster. No amount of insurance can ever replace your data. Once it's lost - it's lost forever.

When balancing cost with security and disaster recovery - be pragmatic. You can't have it all ... but don't stop trying.