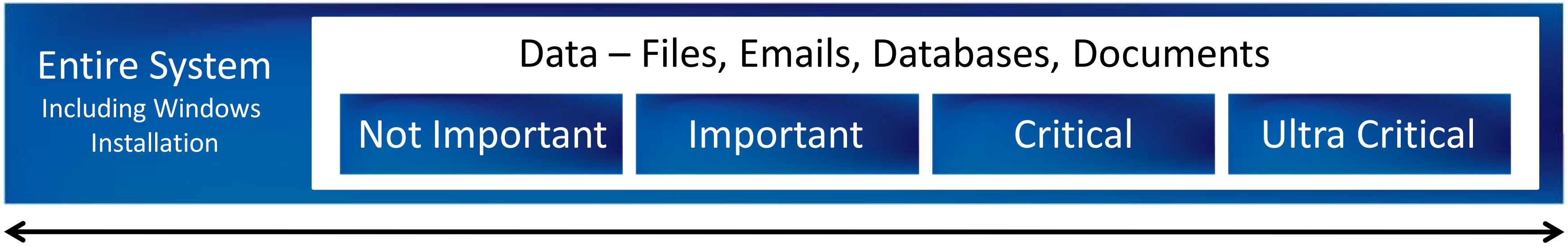
Putting it altogether

- Different backup technologies have different sweet spots.
- How can we design a backup system that best utilises the available technologies?

Types of data



Entire System

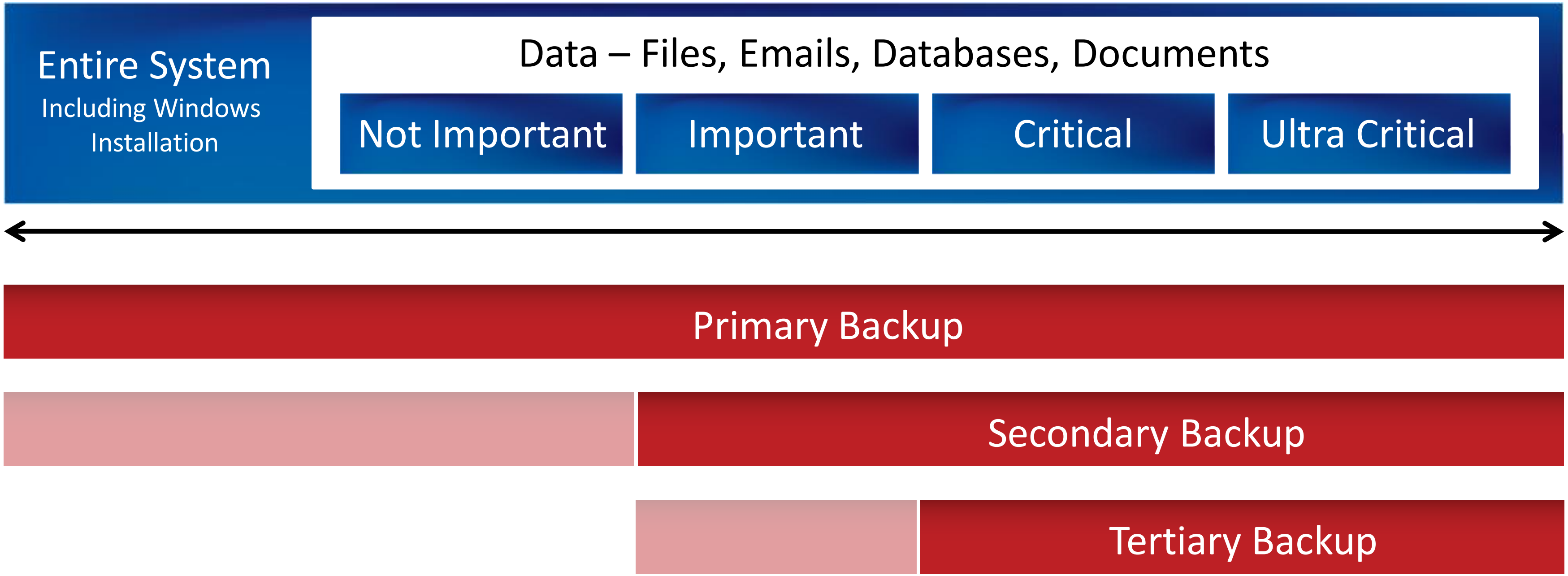
Including Windows Installation

Data – Files, Emails, Databases, Documents

Not Important | Important | Critical | Ultra Critical

Step 1: Look at the data on your server, and decide where each type of data falls into...

Multiple layers of protection



Entire System

Including Windows Installation

Data – Files, Emails, Databases, Documents

Not Important

Important

Critical

Ultra Critical

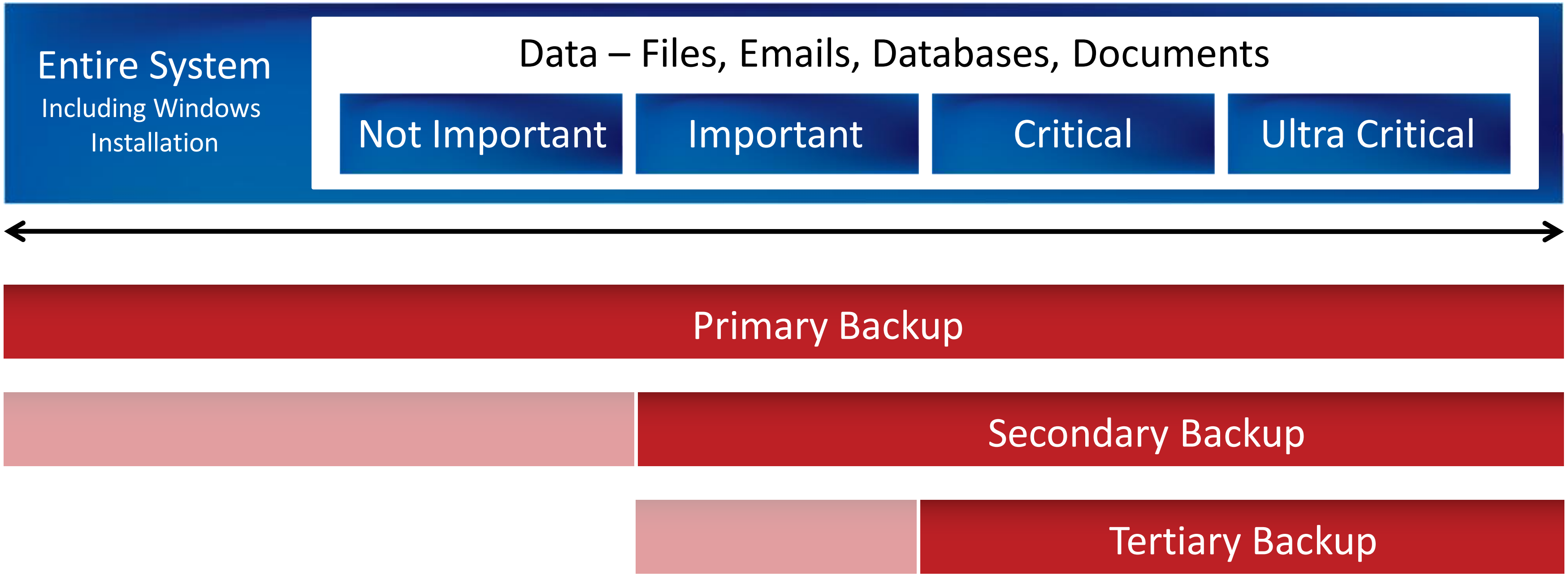
Primary Backup

Secondary Backup

Tertiary Backup

Step 2: Decide how thoroughly you want to protect your data. The most important types of data should get the most protection. We recommend having up to three types of backups for maximum protection against all causes of data loss. Of course, it’s all up to you!

Multiple layers of protection



Entire System

Including Windows Installation

Data – Files, Emails, Databases, Documents

Not Important

Important

Critical

Ultra Critical

Primary Backup

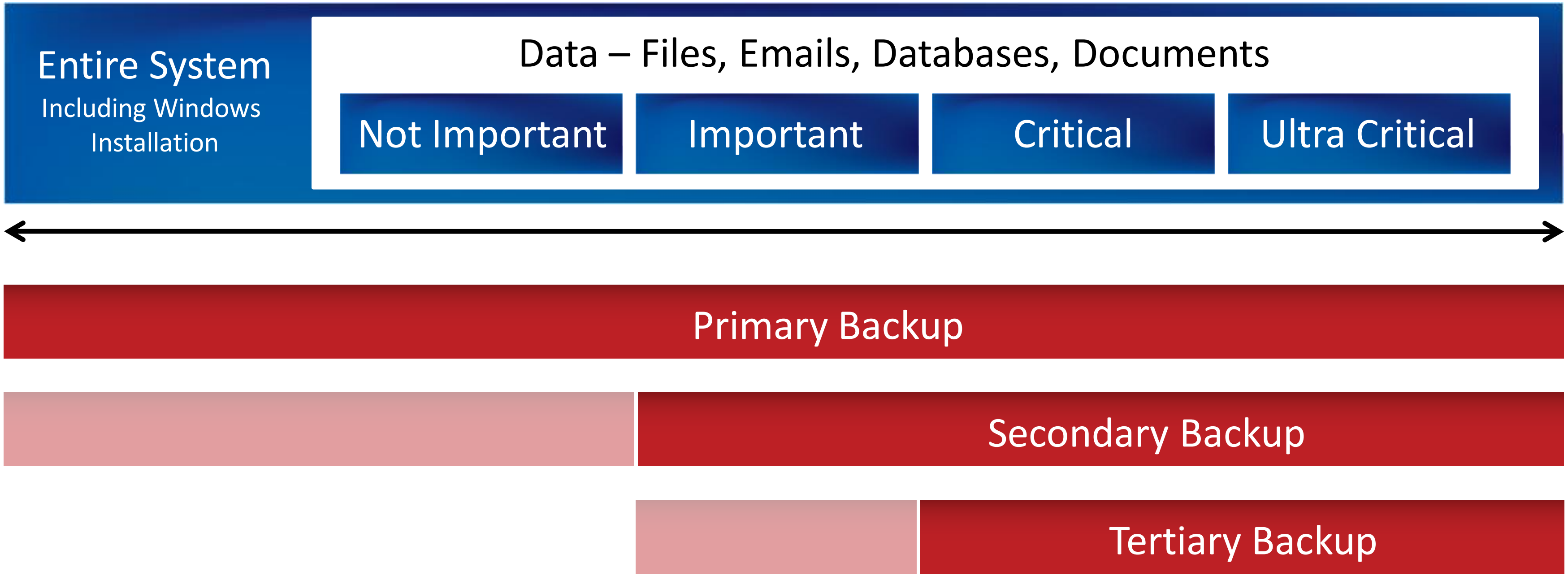
Secondary Backup

Tertiary Backup

Advantage #1: Improved reliability.

If the failure rate of one backup is 5%... The chance that all 3 fail is 0.0125%

Multiple layers of protection



Advantage #2: Flexible.

This model can be adapted to many situations.

Why not do it?

- Reasons not to combine imaging, data archival backup and Internet backup?

Why not do it?

- Reasons not to combine imaging, data archival backup and Internet backup?
  - Need 3 different products
  - Too expensive
  - Overkill
  - Hard to monitor
  - Too complex

Why not do it?

- Reasons not to combine imaging, data archival backup and Internet backup?
  - ~~Need 3 different products~~
  - ~~Too expensive~~
  - ~~Overkill~~
  - ~~Hard to monitor~~
  - ~~Too complex~~

Not anymore!

Example #1a – Manual media rotation

- Primary: Daily drive imaging to USB or eSata HDD – complete server backup to 5 rotating HDDs

Comment: This is the familiar backup scenario, similar to the users swapping tapes daily.

Example #1b – Manual media rotation

- Primary: Daily drive imaging to USB HDD – complete server backup to 5 rotating HDDs

- Secondary: Daily fully automated file system & application backup to NAS or USB connected mass storage

Comment: Dramatic improvement in file system protection... for just a few hundred dollars!

Example #1c – Manual media rotation

BackupAssist™ Windows® Backup Made Easy!

- Primary: Daily drive imaging to USB HDD – complete server backup to 5 rotating HDDs

- Secondary: Daily fully automated file system & application backup to NAS or USB connected mass storage

- Tertiary: Daily fully automated file system & application backup to remote server

Comment: Now protected with automated offsite backups

Example 2 – No client action required

- But what if your client is "lazy" and prefers not to have to do anything?

Example #2a – No client action required

BackupAssist™ Windows® Backup Made Easy!

- Primary: Manual drive image performed by I.T. Specialist as part of preventative maintenance plan, taken offsite

- Tertiary: Daily fully automated file system & application backup to remote server

Comment: Still protected, but not as comprehensively because the secondary backup is missing. Note: The tertiary backup is necessary for up-to-date offsite protection, but restoring all the data from the remote server may be very slow.

Example #2b – No client action required

BackupAssist™ Windows® Backup Made Easy!

- Primary: Manual drive image performed by I.T. Specialist as part of preventative maintenance plan, taken offsite

- Secondary: Daily fully automated file system & application backup to NAS or USB mass storage

- Tertiary: Daily fully automated file system & application backup to remote server

Comment: Far superior in terms of backup coverage and restore speed compared to the previous setup, for just a few hundreds of dollars more

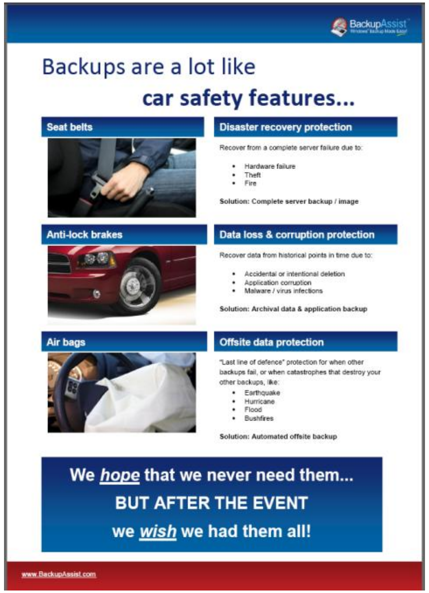
Example #2c – No client action required

- Primary 1: Manual drive image performed by I.T. Specialist and taken offsite
- Primary 2: Daily drive image to NAS / USB mass storage
- Secondary: Daily fully automated file system & application backup to NAS or USB mass storage
- Tertiary: Daily fully automated file system & application backup to remote server

Comment: Better again – now performing daily drive images to NAS / USB mass storage for fast local system recovery, at no extra cost.

Which strategy is right for your client?

- It all depends on:
  - How paranoid is your client?
  - How much are they willing to invest?
  - Your ability to educate your client on the potential dangers.



Backups are a lot like car safety features...

Seat belts

Disaster recovery protection

Recover from a complete server failure due to:

- Hardware failure
- Theft
- Fire

Solution: Complete server backup / image

Anti-lock brakes

Data loss & corruption protection

Recover data from historical points in time due to:

- Accidental or intentional deletion
- Application corruption
- Malware / virus infections

Solution: Archival data & application backup

Air bags

Offsite data protection

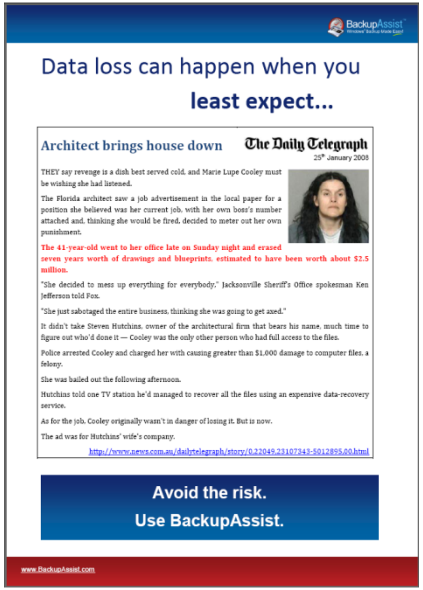
"Last line of defence" protection for when other backups fail, or when catastrophes that destroy your other backups, like:

- Earthquake
- Hurricane
- Flood
- Bushfires

Solution: Automated offsite backup

We *hope* that we never need them...
BUT AFTER THE EVENT
we *wish* we had them all!

www.BackupAssist.com



Data loss can happen when you least expect...

Architect brings house down

The Daily Telegraph
25th January 2008

THEY say revenge is a dish best served cold, and Marie Lupe Cooley must be wishing she had listened.

The Florida architect saw a job advertisement in the local paper for a position she believed was her current job, with her own boss's number attached and, thinking she would be fired, decided to meter out her own punishment.

The 41-year-old went to her office late on Sunday night and erased seven years worth of drawings and blueprints, estimated to have been worth about $2.5 million.

"She decided to mess up everything for everybody," Jacksonville Sheriff's Office spokesman Ken Jefferson told Fox.

"She just sabotaged the entire business, thinking she was going to get axed."

It didn't take Steven Hutchins, owner of the architectural firm that bears his name, much time to figure out who'd done it — Cooley was the only other person who had full access to the files.

Police arrested Cooley and charged her with causing greater than $1,000 damage to computer files, a felony.

She was bailed out the following afternoon.

Hutchins told one TV station he'd managed to recover all the files using an expensive data-recovery service.

As for the job, Cooley originally wasn't in danger of losing it. But is now.

The ad was for Hutchins' wife's company.

http://www.news.com.au/dailytelegraph/story/0,22049,23107343-5012895,00.html

Avoid the risk.
Use BackupAssist.

www.BackupAssist.com

The handouts can help educate your clients!

Revenue opportunities for I.T. Specialists

- Initial sale of hardware and software
- Haas – place a NAS device into client’s network; charge monthly fee
- Internet backup – use your own existing data centre, or buy a server & on-sell space to your client [buy in bulk, resell and mark up]
- Full service monitoring