INFORMATION ESCROW SERVICE VS BACKUP

Digital information continues to expand in quantity and value at an unprecedented pace. The introduction of crypto-currencies such as bitcoin have even expanded it to include digital files that have actual monetary value. Protecting this information has been a requirement since the creation of the very first computer. Historically, this has been the domain of the backup industry. However, all backup systems suffer from the same problem. Even when they work perfectly, they can't actually protect your information.

> **The real problem is that ALL backup systems rely on you to watch your own files. You must notice something is missing or corrupt. It is up to you to run a restore to get the file back. You'd better notice problems quickly enough because the backup system will, by design, delete the last known valid copy of your data.**

How many files can you watch? Of the thousands of files you have, can you detect if something is amiss? Can you tell if you are missing anything right now? These are just some of many problems (disasters?) with today's backup technology that puts your data at risk. The sad fact is that none of today's computing technology, backup included, can actually protect your information.

The Information Escrow Service (IES)

One of the two major capabilities of the Information Bank is its ability to ensure that no matter what happens, you data is safe, protected, and always recoverable. Theft of the bank, failure or destruction of the bank, as well as a long list of other threats can be protected from, mitigated and/or recovered from with the Information Escrow Service. The key attribute of IES is that it is completely hidden and automatic. Much like a financial bank, the user simply "makes a deposit" to the bank and the bank takes care of all the protections and recovery processes without any user interaction. Also much like a financial bank, the Information Bank does not rely on a single technology to provide that protection. It orchestrates the use of over 36 different technologies, with more being added, to ensure your information is protected and recoverable. (See the document on the IES technology list for more details)

The number of technologies utilized as part of the IES implementation is just one difference between IES and backup. Many additional differences outline the huge number of perpetually outstanding problems with backup that are solved, mitigated, or eliminated by IES. The table below documents the terrifying large number of these problems the computing industry has not even admitted to much less addressed in any of their data protection products.

Definition of Backup

There are literally hundreds of backup products available today, each one being slightly different. However, they do tend to fit into some basic categories. One class of backup products scans your file system, detects what has changed, and then sequentially copies your data to some device or service in a serial fashion. Another approach is to monitor the file system and then copy any files as they change. These are often sent to the "cloud" for safe keeping. The comparison matrix below attempts to compare IES with a general view of backup and not specific backup products. We always get some arguments that such-and-such product that we've never heard of does or doesn't do something. That is fine. However, the following statement is still true: None of today's computing technologies can protect your information. Unfortunately, that is the sad fact of the computing industry. IES has been designed to solve such a blatant disaster.

IES vs Backup

The table below is intended to highlight many of the issues with backup and showcase how the Information Escrow Service addresses each issue. People are often surprised by the sheer volume of problems with backup. While any one of these issues could be the subject of a separate dissertation in its own right, the goal here is to simply highlight the quantity of the issues and show they are no longer problems with the Information Escrow Service. Note that the issues are in no particular order.

Issue	IES	Backup	Comment
1. **Protection of your original files that are "backed up"**	Integrated security to avoid the loss or corruption in the first place.	Nothing	Can't currently be done. See the 6-A's of insecurity!
2. **Protection even done at all**	Always on.	Often requires users to run it. Do they?	Often, backup is simply ignored. Too complex and painful.
3. **Restore**	Automatic, unattended, and immediate.	Users must notice. Very unreliable at best.	If users don't see a problem, backup systems do nothing.
4. **Sense of Security**	Absolute. It is monitored, checked, and audited.	False sense	Users have no idea if backup has a copy of everything important to the user.
5. **Modern Design**	Advances the state-of-the-art supplementing today's technology with totally new capabilities.	Many were designed when tape was the only technology available.	Can ancient designs handle today's protection requirements?
6. **Window of vulnerability where changes are not protected.**	Kept to absolute minimum. Files are immediately mirrored and the cloud copy process is initiated.	Some backup systems require you do decide how much work you and your team want to lose.	Ah, I vote zero. Can everyone remember what they did after the last backup? Often a restore can cause more problems than a loss of a file.
7. **Validation of the saved copy**	Automatic	Has no idea what files you are SUPPOSED to have.	Have no way to tell if you have a copy of all your information.
8. **Tell if you're missing anything**	Automatically checked as part of the auditing process.	Have no way to tell	Can't even find out!

9. Response if main and backup copies differ	Can tell which one is valid and will recover the correct one.	Have no way to tell which one is "correct". If the source file is wrong, backup will simply make a copy of the corrupted file, which may be the wrong thing to do!	The correct copy may end up being overwritten or eventually deleted. It is not good to actually have the right copy only to throw it away!
10. Response to a corruption or deletion	The bank can tell the difference and can respond accordingly to ensure the integrity of your information. If the master copy is somehow corrupted, the bank will immediately restore it, log who did it, and sound the alarm.	Backup can't tell the difference. It only knows that the file is changed and should, therefore, be copied.	Backup can't respond correctly in this situation. It relies on the user to notice it and know the difference.
11. Response to ransomware	Resistant to ransomware. All files are set to prevent unauthorized modification.	Ah, you'd better have run a backup! You have to run a restore to recover.	When was the last time it was run? Can you recover all the files?
12. Device renewal	Designed in to support the swap of hardware and storage technology as they become obsolete.	Dependent upon the specific product. Often left out of the product's scope.	Backup device (or service) obsolescence may cause restores from being even possible.
13. Vendor Lock in	Data is always available.	Most products bank on the fact that switching vendors is too painful.	Most users don't change products even after a problem. The devil you know?
14. Switch to different cloud provider	Cloud providers are not perfect and have new and interesting ways to "fail". The bank can change providers without any interaction from users. They will probably not even notice this happened.	Some can but most don't support this.	Cloud storage providers rely on the fact that it is often very painful (and expensive) to switch to another provider.
15. Selection, installation	Already done for you. Not something you have to select or install yourself. Is part of the product.	Users must select and install themselves. Are normal users experienced enough to make informed selections?	Very complex products that are difficult to understand the tradeoffs. Sadly, some users simply ignore backup altogether.
16. Configuration	Always maintains the	Changes in storage	It can come as a real

	configuration so your information is protected.	configuration requires separately reconfiguring backup.	shock to find out someone forgot to change the backup configuration and that new fancy disk drive that broke didn't have any of its data backed up.
17. Verification	The copies made by the bank are always verified and can always be reverified in the future. See auditing.	Backup has no idea what it is supposed to have.	Backup, therefore, has no way to know what it has is correct or complete.
18. Confusing options	There are no options the user must configure. Any potential future options won't put the user's information at risk.	Terms and concepts tend to be confusing to those not in the backup industry. Some backup products try to differentiate themselves on the number of options their products support.	Do you know the difference between a backup set and a backup group? Just what does a user need to understand to ensure their product selection is working correctly?
19. Inventory of contents	Always maintained.	They can keep a list of the files they have but that is of little use if they have no way to tell what they are supposed to have.	Keeping an inventory of that is important and what you should have is a vital part of information management, and yet not supported by backup (or computers for that matter)
20. Copy integrity checks	All file transfers are checked and verified. Should a problem be identified, the copy is restarted and rerun until the transfer was absolutely correct.	While some products perform these checks, others that differentiate themselves by the speed of their backup limit these checks for performance reasons.	File transfers, especially across the internet, are prone to all sorts of interruptions and problems.
21. Sequential Restore	Should individual files be corrupted or deleted, the bank will immediately restore the file. On a complete disaster recovery, the files are restored in order of their importance and done in	Dependent upon the specific product. Some restore only sequentially based upon how it was stored.	Those that have to restore sequentially will restore the 20 cat videos before you can get at your tax records.

	the background. The files that are not yet restored can still be accessed but will be slower since they would need to be copied from the cloud.		
22. Access before restore complete	As outlined in Sequential restore above, once the inventory is restored, all files can be accessed, even if they have not yet been restored.	Dependent upon the specific product.	In a disaster scenario, the sooner your data is available the sooner you can get on with your life.
23. Requires user interaction	Completely hidden and automatic. Requires no user interaction and does not require separate IT staff support.	Some products require more interaction than others. All need to be monitored to ensure they are configured properly, are working, etc.	Any complex technology that requires user interaction is open to all sorts of problems.
24. 3-2-1?	This is a backup philosophy of making three copies, two of which should be on different technologies, one being offsite. The Information Escrow Service is designed from the start to do this.	It is up to the user when selecting, configuring, and operating a backup system to implement such a strategy. Some products would require additional purchases in order to meet this goal.	It can be quite difficult to do this efficiently. Most backup products either don't do this by default or simply can't support it.
25. Loss of cloud credentials	If hackers gain access to your cloud credentials, your information is still undecipherable to them.	Dependent upon the specific product but most cloud-based products will allow a hacker access to all your information should they gain access to your credentials.	Should your information be stolen by a hacker, you may never know it happened.
26. Encryption	This important technology is completely hidden from the user, including any management of the encryption keys.	Most modern backup products do some form of encryption. However, be careful!	See Destination Encryption below.
27. Destination Encryption	Keys are kept in the bank. The cloud services have no way to decrypt your information.	Either 1) they will do the encryption for you or 2) force you to maintain your own keys.	The first is like leaving your key in the lock. Yes, the door is locked but it doesn't stop anyone from turning the doorknob. The

			second is a problem because users must keep the key, which is a digital file, in some way on technology that can't protect your information! Lose the key and all your files are lost!
28. Privacy	Even if someone can access the cloud copy, they will not be able to understand it. The cloud provider can't read your data and sell it to advertisers.	Highly dependent upon the actual product. Some will harvest your information and sell it.	Do you really need more ads shoved in your face?
29. Separate service providers	Four separate cloud services are used to manage your information. Even a compromise of all four services will not make your information decipherable.	Most products that use service providers only use one.	Service providers are known as "high value targets" by hackers.
30. Key escrow	All encryption keys are escrowed in the central bank. The central bank encrypts the keys to protect user information should the central bank be compromised.	Dependent upon the actual product. Most manage the keys themselves putting your data at risk.	Most products will do all the key management for you because they can't trust users to not lose the keys. However, this is also problematic. See Destination Encryption above.,
31. Restores based upon what?	Automatic.	Based upon the name of the file and the directory it happened to be in last. Can you remember these? What if you can't remember what it was called or where it was at last?	These are essentially the last place you put it. Do you know where it was? Users often don't have any idea where it was last or what it was called. Without this information, a successful restore can be a challenge!
32. Search capabilities	Very powerful based upon what the information actually is, not what name and directory you	Dependent upon the actual product. Some only support names and directory searches,	If you can't find something, it might has well be lost!

	happened to place on it.	if they support search at all.	
33. Get the "right" data on a restore	Always.	There is no assurance that the file restored is the actual file and/or version required.	Unless you know the exact filename and directory, the restores might find large numbers of possible "candidates" that you need to sort through. These products can also require several different restore attempts to even get anything that might be a candidate.
34. Know what to backup	Assures that the most recent version is always copied.	Backup has no clue what is important, so they try to backup everything.	Just how many copies of those cat videos do you need to backup?
35. Know when to backup	Context change is the correct time to ensure a protected copy is made.	Ah, on file writes? Too much? When user runs it? To infrequent.	The Information Bank automatically picks the optimal time to perform the mirroring.
36. If a user doesn't detect the loss or corruption of a file.	Watcher does this instantly and triggers the rest of the system to respond accordingly.	If not manually restored quickly enough, the system will delete the last known valid copy of your data.	This is more than a bug. It is a catastrophic design failure!
37. Efficiency	Done when context changes	Depending upon the product, some are so inefficient, it must be run during off hours.	Can lose work. Up to users to remember what they did and redo it!
38. Frequency of backup?	Performed based on the frequency of changes of the information.	Some products will do a backup as soon as a file changes, which many times can be too much. Others wait until you run it, which is almost always not soon enough.	Most products do not allow much control over the frequency of running their product.
39. Directory scanning	Not needed.	Some require a full directory scan in order to tell what has been modified.	Directory scans are a very expensive operation and can cause significant impacts to responsiveness of the computer. And why is

			it that backup, antivirus, and content search all do directory scans at the same time rendering the computer essentially useless?
40. Forensics	All modifications to any Information Asset are automatically logged for later analysis.	Product may log what files they backed up and when but that is of little help to find out what happened to something important.	Backup products cannot tell if they have everything important. Isn’t that the most important thing about backup?
41. Test a restore?	Continuously audited and corrected if problem detected.	Often very difficult.	Almost never done until it is too late!
42. Directional Mirroring	The direction of a copy is always correct. A valid modification causes a copy to be made. An improper deletion or corruption results in an automatic restore.	Some products related to or used for backup such as RAID, mirroring, etc., will simply propagate a corruption.	These products have no way to tell the difference between a corruption and a modification. They always make copies whether or not they should.
43. Disaster Recovery?	Integrated into the bank. A new bank can be restored back to the exact contents prior to the disaster.	Some products can clearly be used for this, but others are not really setup to handle disasters.	You want to get back to your life as soon after a disaster as possible. Are these ever tested?
44. Data breach on backup media?	User information cannot be compromised should any of the cloud copies be compromised.	Dependent upon the destination of the backup. Removable media can be vulnerable without separate encryption. Cloud storage can be vulnerable if credentials are compromised.	The sad fact is that you may not know if your backup copies have been compromised.
45. Designed for-	Everyone. Users don’t have to do anything to gain the benefits of the Information Escrow Service.	Admins, experts, IT, nerds, analysts	Yikes! What are normal people supposed to do?
46. Who has to be taught to do it?	The Appliance	Every user on the planet has to do it themselves.	Really? How’s that been working out?

47. Demonstration	The factory has the ability to disable the individual file security to allow a user to actually delete a file. IES will immediately restore the file. The file manager will only refresh their display after a few seconds allowing the audience to see the file disappear and reappear. This is usually followed by gasps and claps.	Take someone's laptop and tell them you are going to randomly delete files. Watch them freak out!	Please don't actually do this! Yes, it is tragically trivial to trash user's information!
48. Can the technology truly protect your information?	Yes	Sadly, no	The backup industry goes to great lengths to keep this bit of trivia from their customers.
49. Who has the responsibility to protect the information and gets blamed when something goes wrong?	The Bank	You	Yea, not that great is it. I think it is wrong to blame the users for the fundamental problems with backup. Note that in companies, users blame IT, IT blames the backup vendor, the backup vendor blames the user.
50. Automated process controls to keep you out of trouble?	Yes. Just like your financial bank, there are very simple yet powerful processes available.	No clue	Probably the biggest technology restriction limiting any advancement in today's backup products.
51. Significant advancement in information protection over the last half century	Finally!	Pretty much the same since computers were invented.	Most backup vendors are simply not motivated to acknowledge these problems or have the protection process integrated within an appliance.
52. Security Integration	Designed in from the beginning	Most products sort of tacked security on at the end.	Never a good security strategy to add it after the fact!
53. Master Copy Management	Maintains "the" master copy of information.	Users tend to make copies "just in case" and then abandon	Backup has no clue if something is abandoned or not.

		them making the backup quantity worse.	They have to backup all these abandoned copies and will offer them up as potential candidates, often incorrectly, on a restore.
54. All files protected	All files are protected. If they are created or deposited in the bank, they are protected.	Some cloud-based backup systems will ignore certain file types or files that are too large.	These may be very important to you. It can be surprising to find out, often when it is too late, that these were not backed up!
55. Crypto-signatures of each file maintained.	Automatic and hidden. Used to validate the integrity of any copy of the file.	Dependent upon the backup product.	Since no backup system can tell what it is supposed to have, it cannot use these to know which copy is correct.
56. Retention Enforcement	Can be configured as part of the process governing the behavior of the information	Dependent upon the specific product.	Some can keep the copy they have made for a long time, but they can't be sure the copy is the correct data.
57. Destruction Enforcement	Can be configured as part of the process governing the behavior of the information. Can also be setup to ensure no residual copies are left after the destruction.	Dependent upon the specific product.	Some can perform this. Others require the destruction of the backup media. Yet, others have no control over how a cloud provider they use treats removed data.
58. Access to other storage technologies such as archive.	Integrated and done at the process level, not as separate products.	Some include this but most require separate products from separate vendors.	Makes them nearly impossible to integrate and coordinate their operations. The joke in the industry is that every storage feature is its own industry! Each feature you want means you have to buy a different product from a set of companies.
59. Use of deduplication?	All mirrored copies are created with	Some products use deduplication to avoid	Most (all?) of the mirroring and RAID

	deduplication so the total amount of available storage capacity can be used for customer information.	making too many file transfers or copies of the same information.	products require extra capacity, often additional storage devices, to support their capabilities.
60. Based upon the Information Asset Model.	Yes. All the protections are performed with the knowledge that every file is part of an information asset that includes other data as part of that set.	Just file based.	Every current backup product (and all computers for that matter) have the wrong definition of Information. It does NOT match the user's definition.