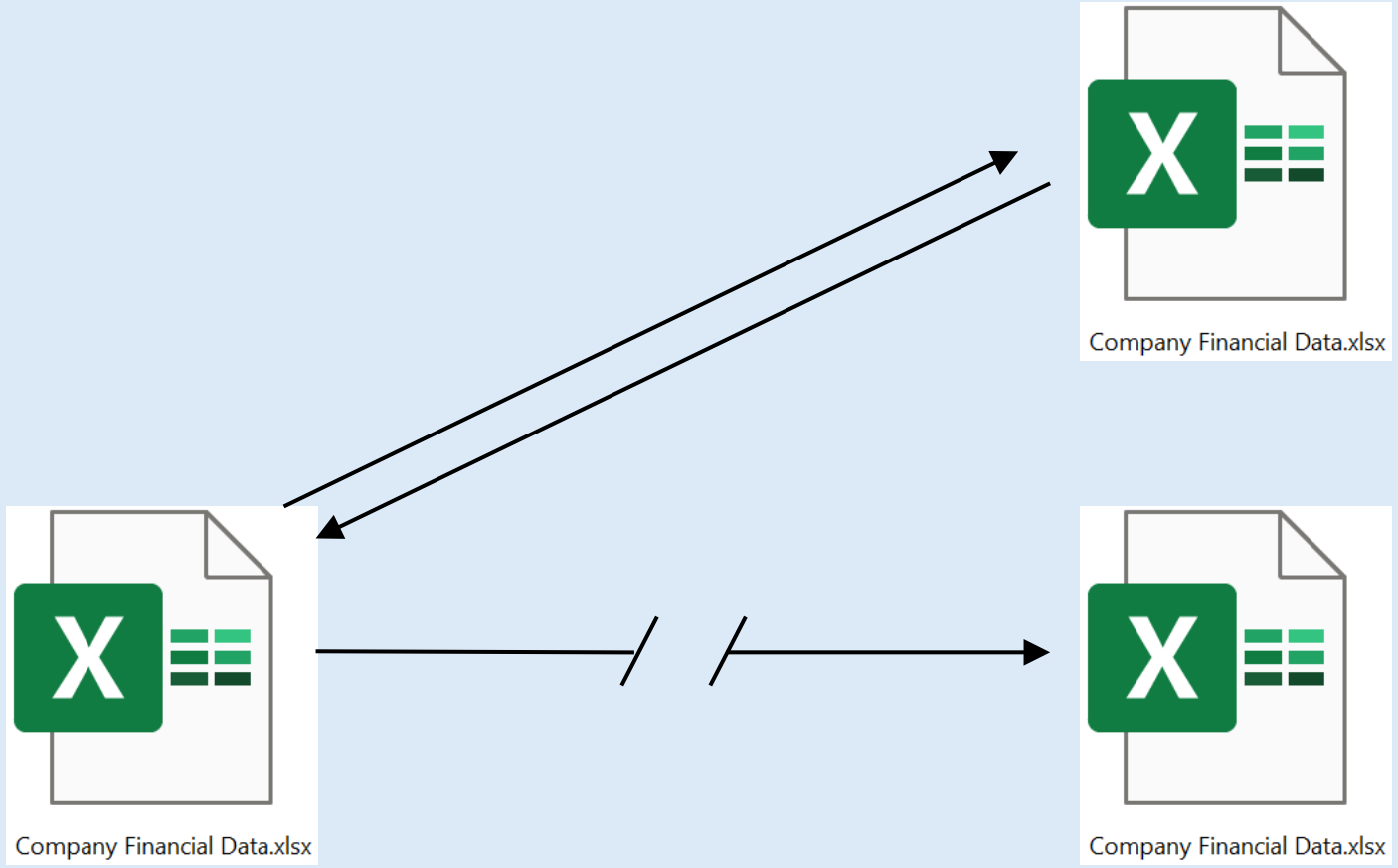
Backup and Sync Explained



ONE COMPUTER WITH CLOUD STORAGE

2) Local app sends synchronized copy to the user's cloud storage account.

Google Drive
OneDrive
iCloud
Dropbox
Carbonite
Adobe Document Cloud
...whatever cloud...

1) User creates document.

The document exists in 2 places. Both copies are identical (synchronized).

TWO COMPUTERS WITH CLOUD STORAGE

2) Local app sends synchronized copy to the user's cloud storage account.

"The Cloud"

3) When there's another computer on the same account, the synced copy is sent to the second computer.

Computer 1

Computer 2

1) User creates document

The document exists in 3 places. All copies are identical (synchronized).

THE 2nd COMPUTER EDITS THE DOCUMENT

"The Cloud"

2) Syncing happens…

3) The updated document is now saved on Computer 1.

Computer 1

Computer 2

1) The document is edited and saved on Computer 2.

The document exists in 3 places. All copies are identical (synchronized).

RANSOMWARE ATTACK!

“The Cloud”

2) Syncing happens…

1) Computer 1 is infected with ransomware and all files are encrypted.

Computer 1

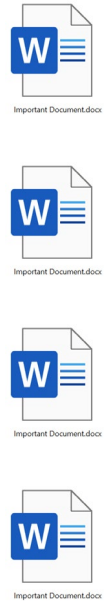
Computer 2

3) Computer 2 isn’t infected, but all synced documents are encrypted.

The documents exist in 3 places. All copies are identical (synchronized), and encrypted.

OLDER VERSIONS TO THE RESCUE (part 1)

2) Local app sends updated copy to the user's cloud storage account.



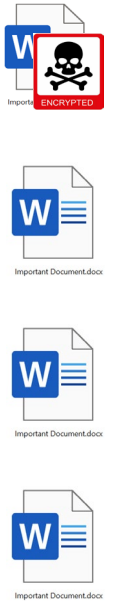
3) Cloud storage keeps the latest version and several older versions.

1) User edits the document.

By storing several older versions the cloud storage provider offers some protection against ransomware.

OLDER VERSIONS TO THE RESCUE (part 2)

2) Local app sends updated (encrypted) copy to the user's cloud storage account.



3) The most recent version is encrypted, but older versions are untouched.
The last "Current Version" is now "Older version 1."

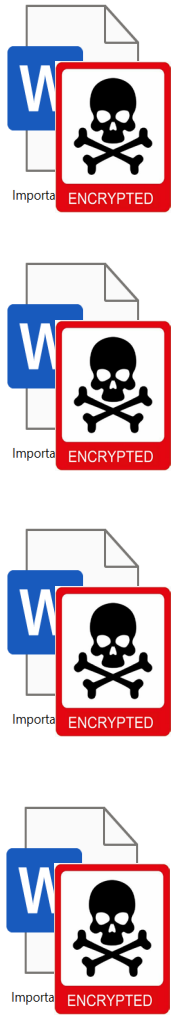
1) Document is encrypted by ransomware.

By storing several older versions the cloud storage provider offers some protection against ransomware.

But there’s a problem…

WHEN THE CLOUD SERVICE PROVIDER IS HIT WITH A RANSOMWARE ATTACK, INSTEAD OF THE INDIVIDUAL USER…

RANSOMWARE ATTACK!!!



ALL of the cloud storage copies are encrypted.

THE INFECTED CLOUD SERVER NOW HAS THE “NEWEST” VERSION OF ALL FILES AND SENDS THEM TO EACH LOCAL STORAGE DEVICE.

Only the server is infected with ransomware.

Computers 1 and 2 aren’t infected, but all synced documents are encrypted.

The documents exist in 3 places. All copies are identical (synchronized), and encrypted.

SIDEBAR

Dropping into “Professor Mode” for a moment, it’s time to explain something to the students that has been tacitly shown, but I want to make sure it’s crystal clear.

Note that in a synchronized environment, the data is encrypted on all endpoints,

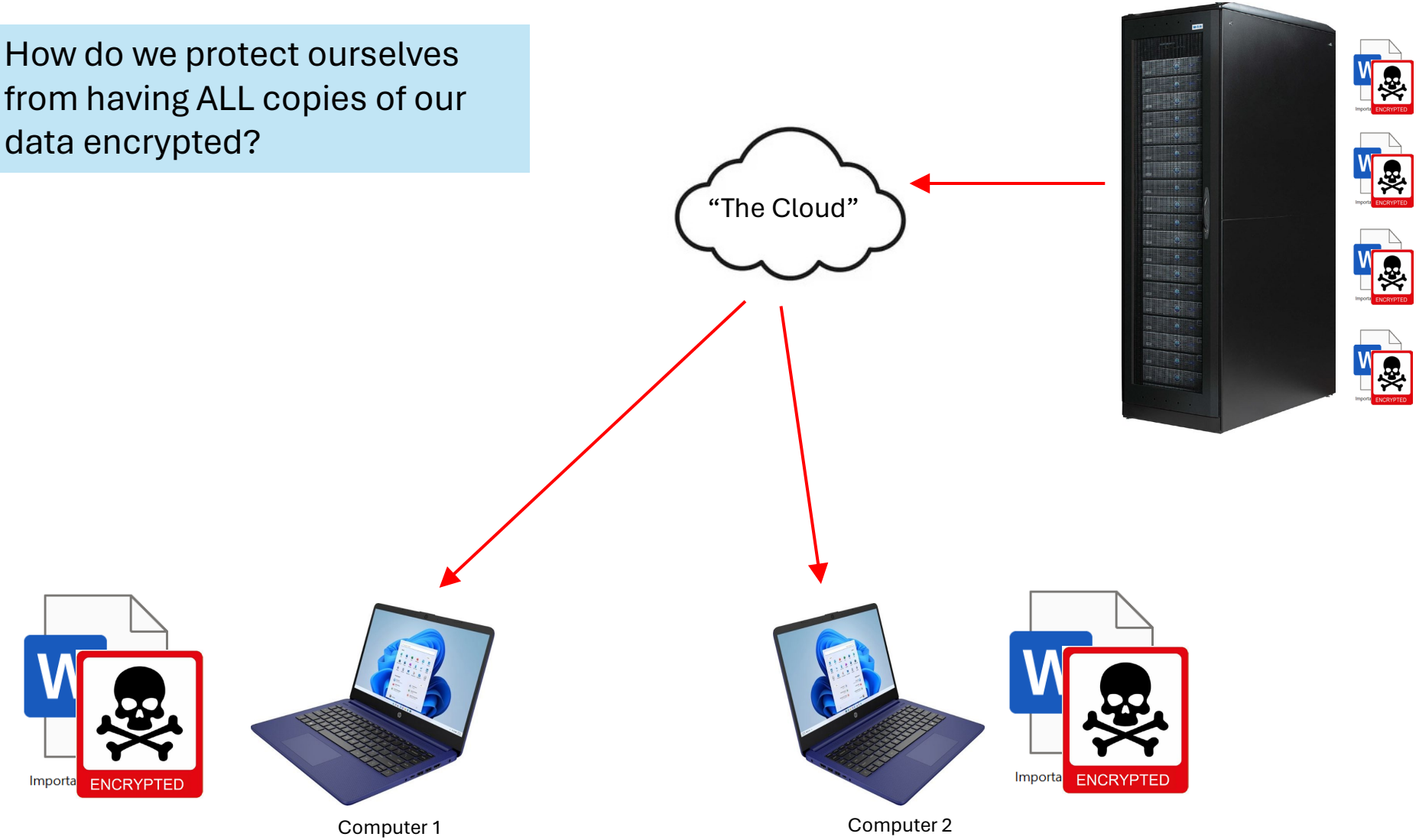
BUT

that doesn’t prove that all endpoints are infected with the ransomware!

It is up to YOU to determine which device (or devices) are infected, and which devices are only repositories for encrypted copies of the data.

And now, back to our main presentation…

How do we protect ourselves from having ALL copies of our data encrypted?



We protect our data by making
FREQUENT
OFFLINE
UNPOWERED
backups.

FREQUENT

Often enough that we can recover and maintain business continuity.

OFFLINE

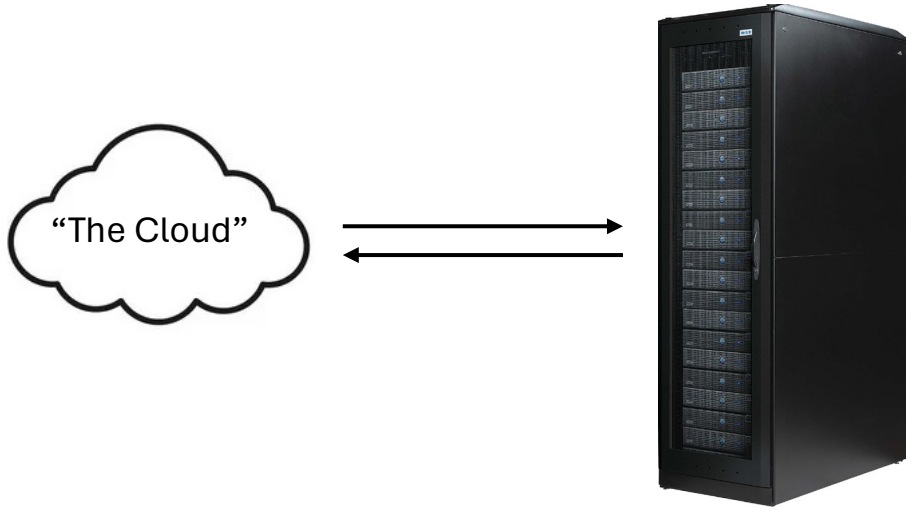
The cybercriminals can’t encrypt offline data.

UNPOWERED

Offline but with power applied? No! If you can bring it online remotely, APT groups can bring it online remotely. Remove power. Manual intervention required.

Wrapping it up…

1. The only correct solution to encrypting ransomware is “wipe and reload.”
2. To do this, you must have good backups.
3. Synchronized “backups” are not backups at all! They’re copies, but not backups.
    1. Whatever happens to one synchronized file happens to every copy – including encryption, corruption, or deletion. They are all effectively *one file*.
4. The Cloud Storage Provider’s historical backups are susceptible to encryption if the CSP is itself the victim of a ransomware attack.
    1. You must take responsibility for your own backup and recovery plan. You can’t blame it on the CSP. You can’t rely on the CSP.
5. Backups that can be used to recover from encrypting ransomware are:
    1. Frequent – data is recent enough for business continuity,
    2. Offline – unavailable to network attacks, and
    3. Unpowered – so the cybercriminals can’t bring them back online remotely.



A word about my representation of “the cloud.”
“Bob, why didn’t you show the server ‘in’ the cloud?”
Because I’m following the historical and original method of drawing cloud architecture. At the dawn of the digital age, as telecom carriers began to provide switched data circuits, the cloud referred to the switching fabric. All endpoints were connected to the cloud, but not part of the cloud. The cloud is the connectivity. It’s only more recently that people have begun to view the cloud as “any part of the Internet outside my building.”
It will help you design and troubleshoot networks if you develop this way of visualizing network endpoints.

Cybersecurity - Networks - Wireless – Telecom - VoIP

Contact Us