How Do I Know My Data is Safe?

Data Safety – Issues and Strategies

Joe Rainero
Robert D'Italia
NetTec NSI and Desktop Co-op

Microsoft GOLD CERTIFIED Partner

Identity & Secure Access
Hosting Solutions
Security Solutions

What is Data?

- Documents
- Communications
- Stored Data (database)

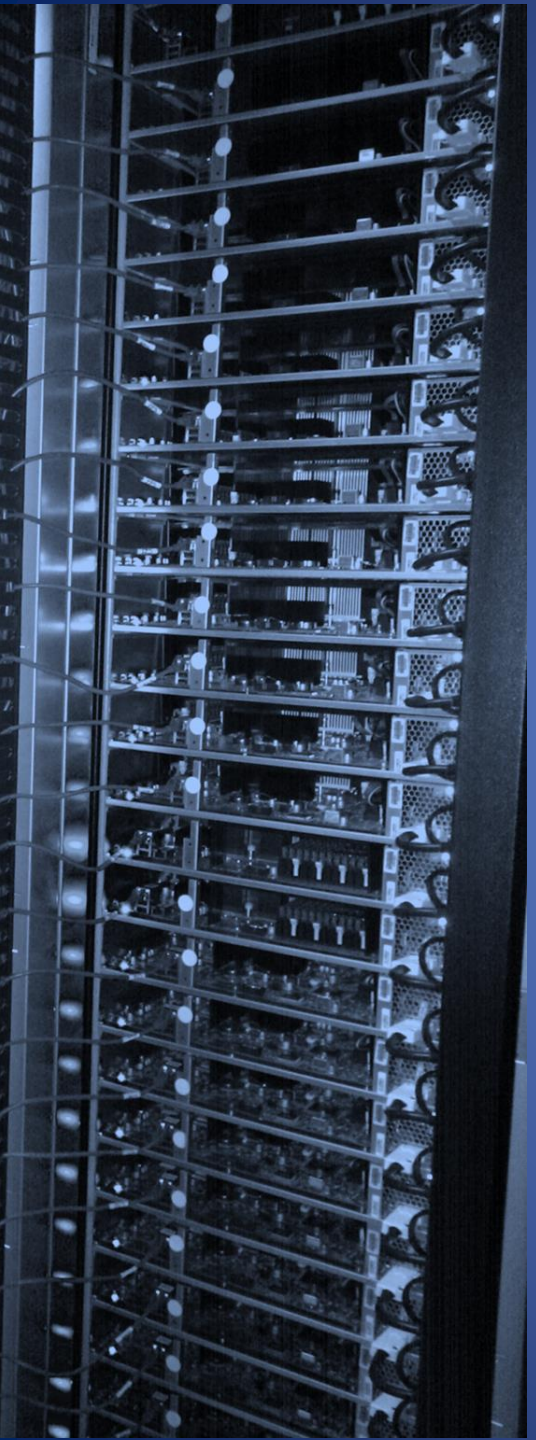
What is “Safe”?

Available
Will be there when it’s needed.

Secure
Available only to those with authorized access.

Recoverable
Can be restored after a disaster.

Availability Strategy: Eliminate single points of failure.



What is Available?

Eliminate single points of failure:

- Power: clean and redundant UPS, generator, utility
- Servers: Drives, Power supplies, Fans, Network Cards
- Networks: switches, firewalls, ISPs
- Backups: local, remote, cloud
- Datacenters
- People: administrators, SOP (printed/electronic), training (video)

What is “Safe”?

Available
Will be there when it’s needed.

Secure
Available only to those with authorized access.

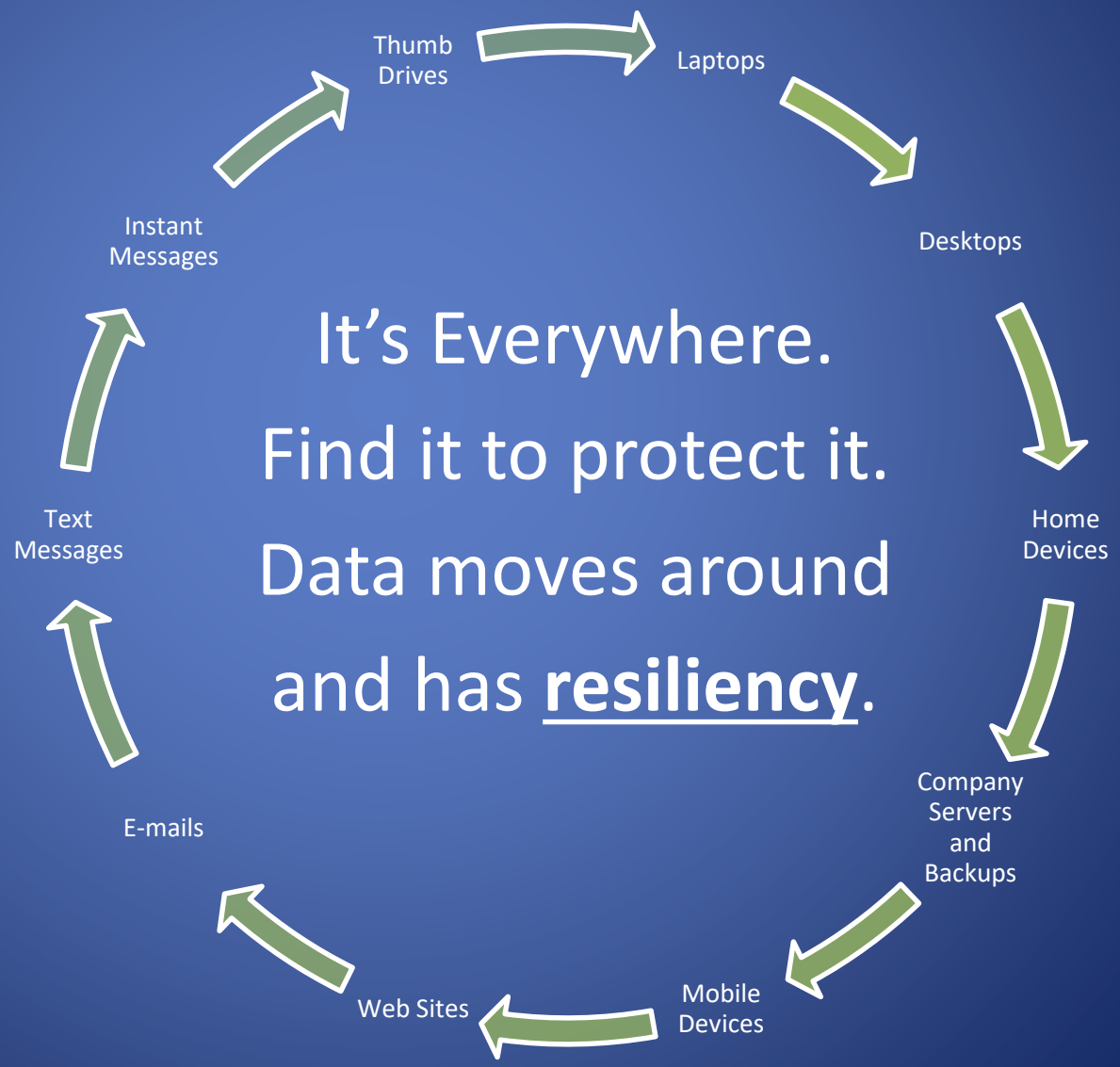
Recoverable
Can be restored after a disaster.

Security Strategy: Control Access.

What is Access?

- Access = Control
- Computers control this with ACLs – Access Control Lists - Who can do what to what?
- Security Tab in Windows
  - It tells who has what permissions: Full, Delete, Write, Read
- There is more to access than ACLs:
  - Physical: data on your computers
  - Network: data in transit.
  - Remote: data stored on the cloud, or across a network like websites, servers, devices out of your control.
- Think about points of access…where is your data? Then think about applying controls.

Where Is Your Data?



It's Everywhere.

Find it to protect it.

Data moves around

and has **resiliency**.

Data Has Resiliency.

- Privacy?
- Today's technology makes it possible to discover anything you do online.
- Just deleting e-mails, browsing history and text messages doesn't really remove the evidence.
  - What information is kept by?
    - ISP
    - Email servers
    - Mobile providers
    - Google Searches = reports of up to 7 years.
    - Facebook = cached pages, Way Back Machine.

Who Has Access to My Data?

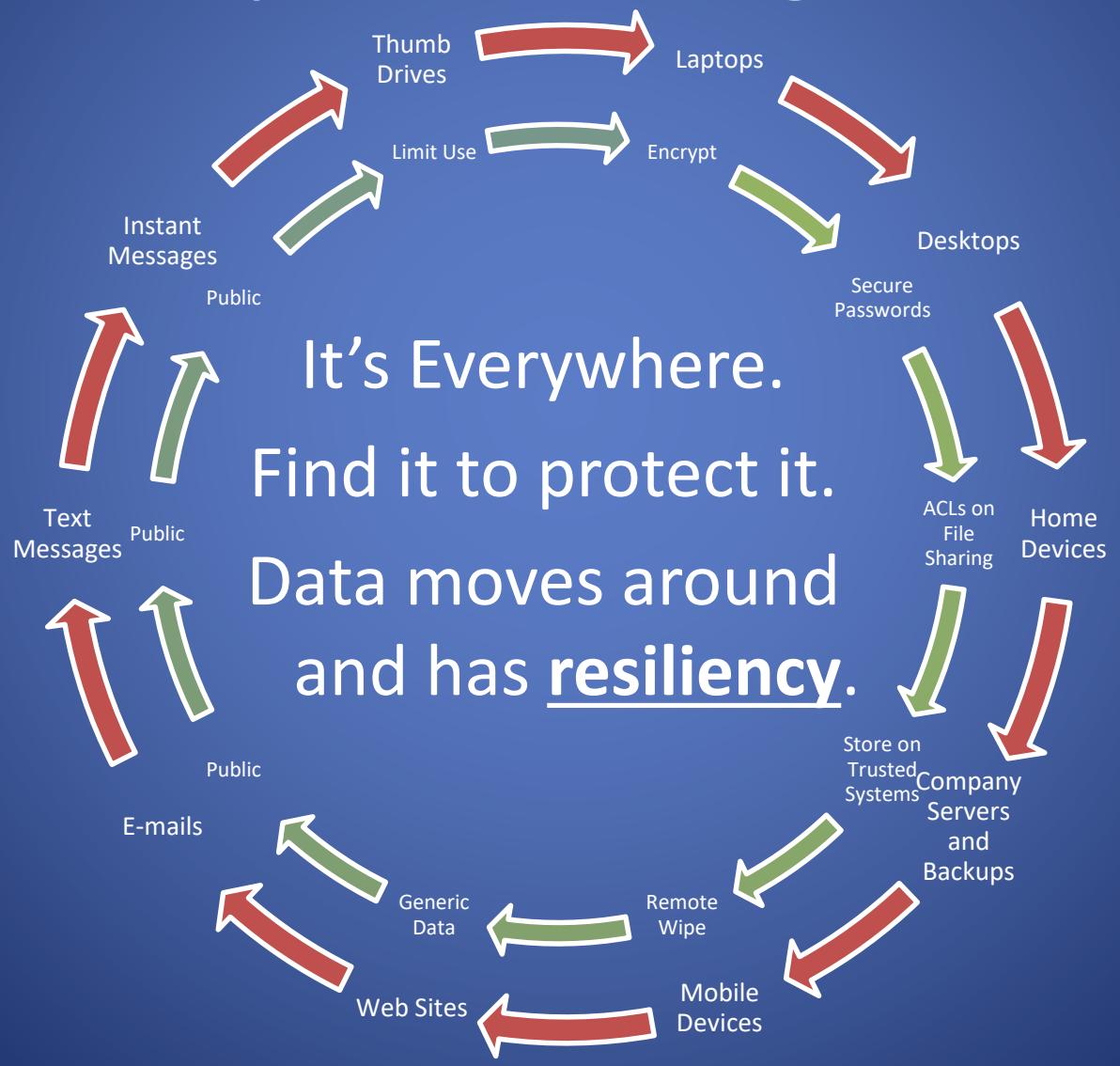
- Systems You Control – Home PC, Mobile Phone, BYOD
  - Kids
    - Windows media sharing and iTunes from game consoles.
  - Housekeeper
  - Baby Sitter
  - Parents – aka your kids' grandparents
  - Neighbors
    - Wi-Fi
- Systems You Use – Work PC, Kiosk, Work Phone (resiliency)
  - Co-workers
  - Administrators
  - Boss
  - Web designer/host
  - Websites - Facebook, web based e-mail
  - Vendors
    - Does your business give remote access to vendors?
    - What do they have access to?
- Key Points:
  - A compromised system gives access to anyone.
  - Physical access gives complete control. With enough time and the right tools, any security can be compromised.
  - Think about what kind of data you want hanging around for anyone to access.
  - Teach awareness.

Strategy: Secure Data by Controlling Physical Access.

Employ strategies to discourage attacks.

- Traditional locks, security alarms, monitoring.
- Carefully choose to whom you give access and use the Principle of Least Privilege: separate user accounts, ACLs, in Windows use standard/limited accounts vs. administrator accounts.
- Drive encryption.
- Limit application execution to a known list.
- Limit failed logon attempts.
- Password protect your data and secure your passwords.
  - Control Panel/Users
  - Don't give them out.
  - Don't write them down.
  - Use a screen saver with a password.
  - Lock your computers using. ⊞ +L
  - When creating a password, create a phrase that only you know and you won't forget; make it simple to remember, hard to guess.
  - Turn on multi-factor authentication (MFA) on everything.
- Protect systems once they're out of your control
  - Auto-wipe and remote-wipe.
  - Clean devices before turning over control – laptops, phones, etc.

Where Is Your Data? Specific Strategies



It's Everywhere.

Find it to protect it.

Data moves around and has **resiliency**.

Strategy: Secure Data by Controlling Network Access.

- Reality – no system is 100% secure if it is connected to something you don't control. To connect and be secure, a level of trust is needed, otherwise go back to about 1960 (pre-Internet).
- You must Protect before you Connect.
- Follow Windows Security Center recommendations: firewall, Windows Update, Anti-malware (free Security Essentials), browser Internet Security set to recommended, User Account Control, conduct frequent and reliable backups.

- Change your Wi-Fi SSID and secure it with WPA2.
- Only use networks you trust and/or control.
- Prevent Compromise: #1 Way - Use Limited or Standard User Accounts in Windows (Control Panel / Users).
- Turn off auto-run on CDs and thumb drives.

Strategy: Secure Data by Controlling Remote Data.

Control what you can on remote systems:

- Use random passwords, not the same on each site.
- Trust no e-mails – SMTP sends in clear text – don't send any personal identity data.
- Encrypt emails
- Use SSL tunneling for remote access.
- Trust no web sites.
  - Use https for web browsing – especially when entering data in a form.
  - Validate the SSL certificate first.
- Use Firefox or Google Chrome as a browser. IE is a target for malware.
- Use OpenDNS instead of your ISP's default DNS servers.

If your Data is Compromised?

- Immediately disconnect compromised system(s) from network.
- Notify key parties immediately:
  - administrators
  - banks
  - webmasters
  - merchants
  - co-workers
  - family & friends
- Flatten compromised systems before returning to use – the only way to be 100% sure you're safe again.

What is “Safe”?

Available — Will be there when it’s needed.

Secure — Available only to those with authorized access.

Recoverable — Can be restored after a disaster.

Recovery Strategy: At least three copies, one off-site with versioning.

It's not 1978…
so stop acting like it.

- **Call PC Safety.** Microsoft provides free malware removal support to Windows customers who think they have an infected computer or have other PC Security questions. Customers should call 1-866-PC Safety for phone support which is available 24 hours a day 7 days a week.
- **Microsoft Safety & Security**
- http://www.microsoft.com/security/default.aspx
- **Applying the Principle of Least Privilege** http://www.microsoft.com/en-us/download/details.aspx?id=4868
- **Microsoft Security: 4 steps to protect your computer** http://www.microsoft.com/security/pypc.aspx
- **Microsoft Security Essentials** http://www.microsoft.com/security_essentials/
- **Microsoft Security: Watch out for fake virus alerts** http://www.microsoft.com/security/antivirus/rogue.aspx
- **Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines** http://csis.org/files/publication/Twenty_Critical_Controls_for_Effective_Cyber_Defense_CAG.pdf
- ***The Top Cyber Security Risks*** http://www.sans.org/top-cyber-security-risks/

Q&A