Available	Issue	Strategy	Details
	Single points of failure	Redundancy	Electric providors
			Uninteruppted Power Supplies
			Circuit breakers
			Power Generators
			Drives - RAID
			Network
			Servers
			Datacenters
			Applications
			People
			Training
			Vendors
	Redundancy is costly	Consider lower cost methods like replication technologies and hosting.	
Secure	Unauthorized Physical Access to Data	Secure areas where data resides.	If someone has physical access, they can gain access.
		Maintain an inventory of all devices where your data resides.	Know what programs are installed and what users have access to these systems.
		Wipe physical devices before discarding.	
	Keyboard Loggers	Physically look for them.	
		Ask who to trust and inspect the system before using.	Only do what you want to be publically known.
	Infected Media	Use up to date Anti-virus	
	CDs, DVDs	Disable Autorun	
	USB (Thumb) Drives	Disable Autorun	Disable autorun, click the lock, format after sharing
	Privacy	Ask who to trust?	Only do what you want to be publically known.
		Use multi-factor authentication (mfa) on all accounts	
		Password protect your systems	
		Use separate, password protected user accounts for PCs	
		Only use limited or standard accounts in Windows	
	Vulnerable Personal Identity Data	Hide in image files with mspaint.exe.	Put the details in random image file and keep its name generic.
		Only provide personal information to those you trust.	
		Password protect physical and electronic access.	
		Use your own code phrases not things like "Mother's Maiden Name".	
	Password Vulnerabilities		
	Easy to guess.	Use a combination of parts of words and numbers that only you know.	Example: 19VTcit97
	Easy to find.	Don't write it down - anywhere.	
	Hacked password recovery.	Use totally made up and bogus information for these.	Do remember this - it will save you when you forget your password.
		Use NOTHING that can be found online about you.	
		Use two factor authentication.	
	Network Threats	Secure connections.	Lock wiring closets and switches physically and electronically.
		Update firewall and network firmware and drivers.	
	Port Scanning	Use Firewalls	Block all unknown and unwanted traffic at the edge and on each inside device where possible.
	Packet Sniffing	Use secure channels for communications - SSL, TLS, VPN	
	Hackers look for open ports.	Firewall between your system and untrusted networks.	
		Only connect to trusted networks.	
	Inadvertant File/Folder Sharing	Check settings in Control Panel Network.	Also check in Computer Management/Shared Folders
		Set Access Control Lists	Also check in Computer Management/Shared Folders
		Check what you're sharing	
	Wireless Vulnerabilities	SSID, WPA2, MAC Filtering	
	DNS Attacks	Secure DNS Servers Externally, Use OpenDNS Internally	
	Unauthorized drive access	Encryption (Bit Locker)	
	Phishing	Use Anti-spam Filters	
		Use browsers with anti-phishing.	
		Use https not http	Check the site's certificate
	Web threats		
	Tracking Cookies, Trojans, bots	Use OpenDNS	Block categories of known bad sites.
	IE multiple vulnerabilities	Use Firefox or Google Chrome	
	Misspelled Domains	Use https not http	Check the site's certificate
		Use OpenDNS	
	Fake Anti-virus alerts	Use Standard Accounts ONLY	Shut down if alerted immediately. Restart as a Standard User and scan.

	Anti-virus 2009, Pro, Whatever	Use Standard Accounts ONLY	Don't trust their fake alerts. Use your own anti-virus to scan or safety.live.com.
	Installation of unwanted software	Use Standard Accounts ONLY	
		Use AppSec, Software Restriction Policies, AppLocker or similar technology	only allows pre-approved software to execute
	Compromised System	Shut down system and remove drive	
		Report Immediately	Alert Admins, Financial Institutions, check corporate policy,
		Flatten system and restore from last good backup.	or…
			Boot to another system and attach drive to scan and recover files
			Reinstall o/s on system and restore files.
	Mobile Device Vulnerabilities		
	Data persistence	Data remains on sender's and recipient's devices.	Only do what you want to be publically known.
	Personal Identity Vulnerabilities	Password protect with automatic wipe.	Available on some devices today.
	Lost device	Report immediately to service providor and admins.	
		Perform remote wipe	Available on some devices today.
	Text Messaging Vulnerabilities		
	data sent in clear text	Only text what you want to be publically known.	Never send passwords, Personal Identity Data, credit cards, etc.
	history saved	Only text what you want to be publically known.	Never send passwords, Personal Identity Data, credit cards, etc.
	some services save local cache	Only text what you want to be publically known.	Never send passwords, Personal Identity Data, credit cards, etc.
	Web Sites		
	data sometimes sent in clear text	Use https not http	
	ISP tracks history	Only surf what you want to be publically known.	This is beyond your control…always be smart when you surf.
	local history and cache saved	Only surf what you want to be publically known.	clear local cache especially of Personal Identity Data or surf incognito in Chrome.
	local routers and servers log history	Only surf what you want to be publically known.	Possible to clear, but can be difficult.
	Instant Messaging		
	data sent in clear text	Only IM what you want to be publically known.	Never send passwords, Personal Identity Data, credit cards, etc.
	history saved	Only IM what you want to be publically known.	Never send passwords, Personal Identity Data, credit cards, etc.
	some services save local cache	Only IM what you want to be publically known.	Never send passwords, Personal Identity Data, credit cards, etc.
	E-mail		
	Infected e-mails	Trust no e-mails.	
		Put a anti-spam filter in front of your e-mail clients and servers.	or have a 3rd party handle your e-mail hygiene.
	E-mail (SMTP) sent in clear text	Only send what you want to be publically known.	You can password protect attachments then send via e-mail (not 100% safe).
		Employ an e-mail encryption system.	Can be on premise or hosted.
	Compromised e-mail	Disable system immediately - unplug from network or shut down.	
		Alert authorities (ISP, Admins, police) and contacts	
		Attempt to recover and then restore services.	
		Implement better methods of provention.	Consider hosting services - better results for the money.
	High costs of Legal Discovery	Implement archiving solution for data (files, databases and messaging).	Consider hosting services - better results for the money.
Recoverable	Must be in multiple locations	File copy	
		xcopy	
		robocopy	
		Script with .cmd and use Task Scheduler.	
		Windows Previous Versions.	
		Traditional backup.	
		Must have a minimum of 3 copies.	
		Store one on-site, one off-site and one in transit.	
		Ask is the process reliable? Only rely on reliable systems.	
		Cloud (internet) Sync.	
		Windows - Mesh, SkyDrive and others.	
		Mac – Mobile Me or Time Machine.	
		Ask – what happens if I delete it accidentally?	