Blue Net, Inc.
Presents

Backup is Good, Recovery is KING
Who is Blue Net?

Onsite Managed Services, Hybrid Cloud and Fully Hosted Cloud Solutions Provider

Proudly serving our clients and fueling success since 2007.
Backup is Good, Recovery is KING!

- Agenda:
  - Common sources of interruptions
  - Common data loss areas
  - RPO and RTO explained
  - Datacenter strategies
  - Manpower considerations
  - Funding and OpEx for Recovery
  - Testing thoughts
  - Where Blue Net fits
Blue Net’s Focus:

VMworld Survey Results of Data Protection in the 21st Century

Blue Net’s Focus: RPO Clients
Targeting “Zero Loss” through “Days”.

Blue Net’s Focus: RTO Clients
Targeting “0 hrs” through “48 hrs”.

Source: http://wikibon.org/wiki/v/Asigra_VMworld_Survey:_Data_Protection_in_the_21st_Century
Blue Net’s Focus (continued):

- **Blue Net’s Focus**: Making Objectives affordable
- **Blue Net’s Focus**: Tested and Proven results

Source: http://wikibon.org/wiki/v/Asigra_VMworld_Survey:_Data_Protection_in_the_21st_Century
Context:

- **Pareto principle**
  - (also known as the **80–20 rule**)

- 80% of potential issues will be taken care of with good design that buys you time to repair without downtime.

- Do you have some level of protection from these? Are you sure?
An old saying:

- An ounce of Prevention is worth a pound of cure.

- Planning to avoid the Friday 4:30 breakdown before the 4th of July weekend...
Some very common sources of outages:

(Organized from the outside coming in on the path of data)

- Backhoes
  - Internet service providers and backhoes don't mix

GRAVES
cause sometimes you gotta dig your own
Some very common sources of outages: (Continued)

(Organized from the outside coming in on the path of data)

- Lightning
  - It’s hard on everything.
  - Power/Data/Voice
Some very common sources of outages: (Continued)

(Organized from the outside coming in on the path of data)

- Wet ground
  - (T-1/MPLS network shorts out)
- Rain and heavy snow
  - Wireless point to point obstruction
Some very common sources of outages: (Continued)

(Organized from the outside coming in on the path of data)

- **Power, power loss or power supply issues:**
  - Everything needs it.
  - Power circuit and breaker failure (a single circuit is common and surge of draw on startup can trip the breaker)
  - Uninterruptable power supply (UPS) undersized, dead battery, fault connected to a single circuit.
  - Critical items not on UPS
  - ISP Router failure (most have single power supply per appliance) (owned by ISP provider in most cases)
Some very common sources of outages: (Continued)

(Organized from the outside coming in on the path of data)

- Power, power loss or power supply issues: (Continued)
  - Firewall failure (most have single power supplies per appliance for small to mid) (most all have HA options)
  - Core switching failure (most have single power supplies per appliance for small to mid) (many have HA options)
  - Servers (most have single power supplies per appliance for small to mid) (many have HA options)
  - Storage and storage networking (some components here have single power supplies per appliance for small to mid) (many have HA options)
Some very common sources of outages: (Continued)

(Organized from the outside coming in on the path of data)

- Heat
  - Protection isn’t just needed in the datacenter.
  - Also Evaluate:
    - Demark Location(s)
    - Switch Closets
    - Edge Site Closets
    - Critical users offices
Recap Hardware and Internet Service Provider (ISP) Redundancy:

- Good design, hardware planning, engineering and lifecycle management gets around these single points of hardware failure.
- IF YOU CANT AFFORD TO DO THIS CORRECTLY ON SITE, WITH A LEVEL OF THIS: HOST THE CRITICAL APPLICATIONS.
Data loss and corruption:

(Organized from some of the most common)

- MICROSOFT!!! (and other OS’) patches and updates breaking applications.
- Test, retest and test more in a "pilot stage" before a "mass production rollout stage".
- AT THE VERY LEAST HAVE A "BACK-OUT PLAN".
- Modern storage and server operating systems and Storage have these options if your licensing correctly and have this "user productivity" centric focus.
Data loss and corruption: (Continued) (Organized from some of the most common)

- Application updates have the same issue as MICROSOFT...
- Test, retest and test more in a "pilot stage" before a "mass production rollout stage".
- AT THE VERY LEAST HAVE A "BACK-OUT PLAN".
- Modern storage and server operating systems and Storage have these options if your licensing correctly and have this "user productivity" centric focus.
Data loss and corruption: (Continued)

(Organized from some of the most common)

- Poorly written software can corrupt data.
- You will not know you have this vulnerability until you face data loss. Have recovery option(s)!
Data loss and corruption: (Continued)

(Continued)

(Organized from some of the most common)

- Bad power, bad memory, bad firmware, bad motherboard and HD failure can corrupt data. These items can be working fine one moment, then break and take data integrity with it. Have recovery option(s)!

- HD failure. Many MANY options for hard drive protection are available. The amount of performance and the amount of storage you require plus the level of hard drive protection features will equal your pricing level. Keep in mind corruption can still occur on the running operating system and applications. Have recovery option(s)!
Back to the **Pareto principle** (also known as the **80–20 rule**...)

- Congratulations! We just covered 80% of issues!
- Let's talk about the remaining 20%
- The remaining 20% are the most costly.
80-20 Rule applied to remaining 20% in the first 80–20...

- After good system design and investment into each site’s stability we get to issues were it starts to get interesting.

- Lets talk about the remaining first 80% in the remaining 20%... (16% of the Initial Quantity)
System Uptime and Loss of Data Access:

- #1 Cause of Trouble: ??
System Uptime and Loss of Data Access:

• NOT Viruses and Hacks...
  • These are concerns to be taken seriously!
System Uptime and Loss of Data Access:

- **Not Malicious Employees...**
  - A Real issue and a whole presentation on data loss due to Malicious Employees and the measures that can be used to protect you from them could be done...
The #1 Cause of Trouble with Loss of Data Access and System Uptime

- #1 Cause of Trouble = Accidental Employee Data Loss or Mistakes
80-20 Rule applied to remaining 20% in the first 80–20...

- After Accidental User issues, Malicious Employees and Virus and Hacks. We get to Catastrophes.

- Lets talk about the remaining first 20% in the remaining 20%... (4% of the Initial Quantity)
Catastrophes are RARE!!

- Not Everyday do we have a true Catastrophe!
- We do have some interesting issues and it’s worth planning for...

Downtown St. Paul water main rupture floods streets; residents asked to boil water

By Will Ashemacher and Kraig Odden
Pioneer Press
Posted: 02/09/2013 12:01:00 AM CST
Updated: 02/09/2013 08:34:15 PM CST

Duluth flash flooding destroys roads, leads to zoo animal drownings

Flash flooding in Duluth, Minnesota, has forced residents to evacuate, left homes underwater, destroyed roads and even led to the drownings of at least eight...
Business Continuity planning looks at RPO and RTO holistically.

- Consider ALL mentioned above as we get into the RTO and RPO conversation.
Backup, Disaster Recovery and Archiving are separate topics!

- Recognizing there is a difference, your needs and strategy can save you money here.

- Example: A Disaster Recovery site for Business Applications may not have Archiving. The Archiving is at the Primary Site and offsite in a low cost bulk storage solution.
RPO and RTO

- Recovery point objective (RPO) (“O”= objective... not mandate)
- Recovery time objective (RTO) (“O”= objective... not mandate)
- These two metrics describing the limits of acceptable or "tolerable" performance in terms of time lost (RTO) from normal business process functioning, and in terms of data lost or not backed-up during that period of time (RPO) respectively.
Zero is Costly

- The tighter the window around an event; the more it costs in automation and system overlap to push toward Zero downtime/Zero loss.

- RPO and RTO needs are getting shorter and shorter for everyone as we are building in more dependencies on technology.
The shorter the time, the more it costs!

- This is due in part to the amount of automation and complexity for sites to be available for the internal and external needs with little or no user issues.

- **Correctly** providing on premise redundant power and cooling are generally out of the questions for even small and midsize enterprises.

- Cloud Services and Hosting have taken RPO and RTO and put lower time frames within reach of all companies.

- Software as a Service offerings generally come with redundancy measures as part of the cost. *(Is your internet 100% solid so you always have access?)*
RPO and RTO applied to the workforce:

- You may consider applying RPO and RTO principles to technology users.
- Do you know the costs for one employee to be having IT issues with their desktop or laptop hardware for one day?
- How many employees have issues each month?
- What is that costing your organization?
- Would this justify better tools, an extra tech or a shift to advanced technology or a better solution?
Have a Primary and some kind of Secondary Datacenter!

- Singular Datacenter
  (Not a good option!)
  - Surprising how much of this I see.
  - “We have very few issues”...
  - Even organizations facing compliance and reporting requirements.

(You’re willing to risk it? WHAT? REALLY?)
Datacenter Options:

- Active/Passive Datacenter
  - Systems at a branch office generally part of a lifecycle plan.
- Managed Backup Solutions (Easy and Affordable)
- Cloud or Collocation options

- Ready and waiting
  - Full or Partial Recovery
Datacenter Options: (Continued)

- Active/Active DC’s
  - Systems at Datacenters
  - Critical Systems duplicated fully
  - Some systems may strategically be isolated
  - Cloud or Collocation options

- Ready and waiting
  - Full or Partial Recovery
Blue Net’s Hosting Net Diagram Example:
Datacenter Options: (Continued)

- **N+1 DC’s**
  - Datacenters all over the US or World ALL ACTIVE with enough horsepower to suffer a loss of one DC, with little or no impact to users.
  - Advanced Automation, DNS and Server Load Balancing for fastest responding resources.
What type of Datacenter scenario is right for me?

- Compliance and reporting requirements
- User and online revenue demands
- If you’re looking at Active/Active you should be also planning on N+1 in the future. (They use similar tools)
- Ongoing funding

---This is an Executive or Board Level Decision! I.T. will have it’s part to play, but at the core this is a leadership decision that needs backing and funding.
Manpower considerations during an emergency to execute:

- Some organizations, like manufacturing, have the mantra “if we lose this facility we can’t continue to make our product due to the specialized equipment we have here”. “That is what business risk insurance covers”.

- 93% of companies that lost their data center for 10 days or more due to a disaster filed for bankruptcy within one year of the disaster. 50% of businesses that found themselves without data management for this same time period filed for bankruptcy immediately. (National Archives & Records Administration in Washington)
Manpower considerations during and emergency to execute (continued):

- Redundancy for I.T. systems insures that your team can communicate, access customer data, business data and “fill in the blanks” so that recovery from an issue is rapid.

- In a true catastrophe consider that employees have also been personally affected and family will always come first to most. So what then if your IT personnel, CFO, Key operations teams don’t report to work?
Manpower considerations during an emergency to execute (continued):

- Who needs to fill the roles and get things back up and running?
- CFO’s are often the top tier of the IT Organizational Chart.
Human Bandwidth:

- Having a plan
- Building relationships to support plan
Funding and OpEx options for Recovery Systems

- Having a proven, tested and advanced business continuity plan can be a measurable cost savings to your business Risk Insurance.

- If you're not proactive and documenting this, will the Risk Insurance company and their underwriters find a loophole and not pay?
Funding and OpEx options for Recovery Systems (Continued):

- Higher performance systems for more performance and more transactions day to day and during a fault scenario.

- Day to day user environment enhancements with Virtual Desktops and protections from data loss or Data Breach. Employee mobility and efficiency enhancements.

- Regulatory compliance and protection against data-loss or data breach within a secure environment.

- Secure and revocable access to data when an employee leaves or is let go.

- Power and Energy savings and rebates depending on your current systems status.
Your Continuity Plan needs to fit your budget ongoing:

- A fine line of what risk your business can accept and what critical systems needs to be available is defined only when you really start to plan this out.

- This is an ongoing investment in-house or hosted.
TO OFTEN I.T. STAFF TAKE IT UPON THEMSELVES TO BE CHEAP, INSTEAD OF STRATEGIC.

- Some IT professionals “make it work” instead of working toward the broader business goals.
- Evidence of this is no uniformity in system components
- No detailed lifecycle plans
- No detailed Software maintenance renewals and support contracts
- Few strategic partners for planning if any
It’s not that difficult, it just takes planning!

- Engage with good partners willing to have the depth of conversation this subject requires.
- Gain insight from your internal teams on critical items from their perspective, you will be surprised.
TEST IT!

- DR strategies and fault tolerance planning requires testing.

- Pull the plug
- Pull the controller
- Pull the power supplies
- “Cut” the ISP
- Etc, Etc...

- RECOVER! FAIL OVER! Weekly, monthly... as often as you can.

- Some systems mount and automatically provide evidence of their readiness to be used as a Recovery point daily (or as often as you want this proof).
Blue Net Consulting and Services

- **NO PERSON IS AN ISLAND**
  - We add experienced personnel to your team.

Big Data-specific applications

Infrastructure to make it work

Something to keep in mind
Blue Net Consulting and Services

THE 7 LAYERS OF OSI

PDU (Protocol Data Unit)
(units of data passed between layers)

Transmit: Term for a unit of data at this layer

Receive: Term for a unit of data at this layer

Open Systems Interconnection
Where IT Professional Need to Focus

USERS

PLANNING

Your career with thank you!
Blue Net’s Value Add for IT Professionals

Layer 8
Users
(Sometimes called layer 8)

Layer 7
Application layer
Layer 6
Presentation layer
Layer 5
Session layer
Layer 4
Transport layer
Layer 3
Network layer
Layer 2
Data link layer
Layer 1
Physical layer

Layer 0
Planning/Consulting/Expertise

Area #2:
Where You Should Focus
SPEEDS,
FEEDS,
BITS &
BYTES

Area #1:
Where You Should Focus

Partnership
Where Blue Net Fits:
Onsite and Offsite
IT support for
Systems and Users
Hosting on Pre-
Built Hyper
Redundant
Systems
Planning/
Consulting/Expertise

BUSINESS SUCCESS

Where many IT professionals spend WAY too much time
How Blue Net goes to market

Ticketing and Auditable report of all work performed
  Blue Net Engineering
  Blue Net Triage
  Client Advanced Team Sharing
  Blue Net’s Advanced Tools
  Client Advanced Team Escalates to Blue Net

Blue Net Routine Engagement
  Blue Net Monitoring
  Blue Net System Tools
  Client Helpdesk Team

Level 3 Critical Planning/Testing/Expert

Level 2 Advanced Work/3rd Party Application Management/Upgrades

Level 1 Baseline/User Support/Routine Work/Updates
Why Blue Net?

- Business Continuity is a process that takes ongoing effort and consistent planning.
- Blue Net may not get every tangle out the first time, but with ongoing effort we can bring alignment to Expectations and your Reality.
Arlyn Wall
Senior Solutions Advisor
awall@bluenetinc.com
Cell: 320-420-4794
www.bluenetinc.com