IT Assessment Report

Prepared by:
Date:

BRI Works
www.bri.works
321 East Main Street, Suite 200
Charlottesville VA 22902
434.951.7979

Table of Contents

Executive Summary……3

IT Summary……3

Assessment Goal……3

Assessment Procedure and Scope……3

Assessment Summary……4

Assessment Detail……6

Backups……5

Switching/Cabling……7

Wireless……8

Firewall/Router……9

Internet……10

Workstations……11

Server/NAS……12

Email……13

AntiVirus……14

Licensing……15

Physical Environment……16

Policies and Procedures……17

Action Plan Summary……18

IT Summary

The IT environment that supports [COMPANY] comprises three office spaces in 2 buildings. There is a point to point connection in place with all Internet traffic going in and out of a soon to be leased out location as [COMPANY] has outgrown the original office space. The initial IT infrastructure was configured by BRI Works for a user count of 10-15 in 2009. Subsequently an IT Director was hired and has been supporting the growing infrastructure to a user count of 55 in 2013. There are two physical Windows servers in place supported by various switches, access points, a NAS, Mac mini, and Cisco firewall. There are a mix of Windows and Apple workstations. Email is hosted and backups are stored remotely. These conditions are typical with a small to medium business, especially one that has grown as successfully as [COMPANY].

Assessment Goal

[COMPANY] is currently auditing its IT environment to ensure it does and can continue to optimally support its business goals. [COMPANY]'s stated IT and IT Assessment goals include:

- Stability – IT infrastructure and policies to minimize disruption.
- Efficiency – Achieve efficiencies in that come from stability.
- Risk Analysis – Review IT Systems and procedures for current opportunities for improvement as well as facilitating future growth.

Assessment Procedure and Scope

BRI Works utilizes network tools, [COMPANY] documentation, direct observation, and interviews to review an IT environment. BRI Works has a do it right mentality versus a just make it work approach. BRI's aim is to minimize risk and to validate that BRI Works identifies risks and opportunities for improvement with a traffic light system that flags observations as green, yellow, and red.

GREEN	-	From no to mild risk – no immediate issues and/or minimal consequences
YELLOW	-	From mild to medium risk – will require attention in the next 3 months and/or not aligned with best practices.
RED	-	From medium to urgent risk – imminent issue and/or serious consequences

Throughout each of the 12 areas reviewed in the Assessment, BRI targets 3 core pillars that we call SMB IT:

- Secure IT – Can it be secured and how do you know it's secured?
- Manage IT – Can it be managed and how do you know it's managed?
- Back IT up – Can it be backed up and how do you know it's backed up?

The scope of this assessment was for [COMPANY] internal IT only. There is a public website and publically available servers, social media, and a phone system that are not accounted for in this report, but are opportunities for future review. For the purposes of this report, the term workstation refers to desktops, laptops, tablets, and ultrabooks.

Assessment Summary

BRI Works therefore offers this IT Assessment in order to provide suggestions on how the IT environment could be enhanced to better support these business goals.

In general BRI Works' IT Assessment found that the current IT infrastructure, support model, processes, and procedures are basically supportive of the current business needs. Parts of the infrastructure where [COMPANY] does not have a subject matter expert are supported in a reactive nature and some necessary processes and procedures are undocumented such as onboarding processes and disaster recovery plans.

As with any IT infrastructure, there is always room for improvement. Areas reviewed and their flags are listed below:

RED	Backups – Possible discrepancies with what needs to be backed up and what is actually configured to be backed up.
YELLOW	Switching/Cabling – Unmanaged switches present in some open workspaces and some unsupported switches in network closet.
YELLOW	Wireless – Multiple access points possibly conflicting with themselves without a single dashboard view to manage them.
RED	Firewall/Router – Current firmware level is circa 2009 with known vulnerabilities.
GREEN	Internet – Fiber, business grade connection in place.
YELLOW	Workstations – Some company data is stored on local workstations and no reporting/management for laptops when not in the office network.
RED	Server/NAS – No hardware RAID on one server and external DNS zones hosted internally.
GREEN	EMAIL – Cloud hosted email with a major provider.
YELLOW	AntiVirus – No reporting/management for laptops when not in the office network.
YELLOW	Licensing – Fully up to date and centralized repository is not present.
YELLOW	Physical Environment – Non-IT staff has access to equipment. Lack of ventilation and temperature management, sink in network closet, and temporary chain locking doors.
RED	Policies and Procedures – Some best practices documentation and procedures are not in place, such as: IT contracts, onboarding process, disaster recovery plan, hardware and software lifecycle plan, and network use policy.

The following pages focus on each of these areas listed above and provide detail about specific improvement needs identified. BRI will provide quotes and estimates for remediation and optimization based on the outcome of discussions for the report.

In addition to identifying these recommended improvements to the IT infrastructure, BRI is also able to help remediate these issues. However, [COMPANY] has the option of using any qualified IT provider to assist with their IT environment.

Blue Ridge InternetWorks thanks [COMPANY] for allowing us to perform this IT Assessment. We trust that it will be valuable to you as you decide how to ensure that IT supports your business goals.

Assessment Detail

Backups - RED

Jungle Disk is remotely backing up data to the cloud. It is not known if all company critical data is configured appropriately to be backed up. There is a current project in progress to migrated data from the server to the NAS. Backup jobs will need extra attention throughout this process to minimize inadvertent data loss. While Jungle Disk is part of Rackspace, a company well known for hosting; BRI has not evaluated their customer response level, support model, and restore capabilities with regard to remote backup. Disaster recovery is noted in the Policies and Procedures area. Remote backup is one of the most cost effective offsite backup solutions available. There is no local backup in place. There are certain scenarios where a large data restore is needed and a local backup would minimize the time to restore. Depending on [COMPANY] preference a hybrid solution can provide the most flexibility.

Action - A thorough audit of backup jobs is recommended to ensure just because a job completes successfully does not mean all required protected data was backed up.

Action – Confirm support model meets [COMPANY] expectations.

Action - It is also recommended that routine restores are tested to confirm backups are working correctly.

Optional Action – Configure a form of managed local backup can be configured to shorten restore times for large amounts of data if needed.

Switching/Cabling - YELLOW

Cabling has previously been performed by a BRI approved contractor. Cat5 minimum rating cables run from wall ports to business grade patch panels. The cabling appears to be managed and labelled appropriately, but there is not enough of them. There are multiple unmanaged switches at some users' desks. These can cause performance issues for the end user and even affect the whole network's performance.

Action - It is recommended that each device needing wired connectivity be professionally cabled by certified wiring contractor to reduce end user issues and keep network management in network closets away from workspaces.

Action – Remove unmanaged switches and confirm devices successfully connect to wall ports installed in previous action item.

There are two Cisco Catalyst 2950 switches that are beyond 5 years old and not under warranty. However, given that the first floor Monticello office is going away, it may be possible to set one switch aside as a spare. If any issue arises, Cisco will not be available for support calls, so there is still risk associated with the spare scenario. The 2950 switches also operate at 10/100MBps speed connections and are slower than the other newer Cisco switches in the other offices that run at 1000Mbps speed. All managed switches are appropriately connected to battery backups to ensure stability and longevity of hardware.

Action - It is recommended that they be replaced with newer, faster, and up to date switches covered by warranty for security, speed, and stability.

Alternative Action – Bypass hardware replacement and use one switch as a spare for the other saving on immediate hardware costs but not using faster and more secure new switches.

Wireless - YELLOW

Public Wi-Fi is not provided, saving the overhead of managing performance and security for that vector. Business grade wireless devices are currently in place, but they are not cloud managed and are not in a mesh style network; meaning users may bounce from one access point SSID to the next and experience some delay in that transition. [COMPANY] has already begun the path to cloud managed wireless by means of a Meraki webinar. Meraki has been BRI's Cloud Managed Networking vendor of choice since 2007 and in fact BRI managed Meraki access points serve as the backbone to Charlottesville's Downtown Mall Wifi among other numerous implementations. The devices also have the built in capability for segregated guest Internet access should the need arise in the future. The access points are appropriately connected to battery backups to help ensure stability and longevity of hardware.

Action - It is recommended that all access points are transitioned to centrally managed devices for cloud management in a single dashboard allowing users to better monitor, manage, and access the network.

Action - It is further recommended that the security access settings are changed on a regular basis as part of best practices security measures.

Firewall/Router - RED

The firewall firmware hasn't been updated since the year 2010 and the memory available only supports to a 2011 version of firmware. There are publically known vulnerabilities for the version on the firewall. The router is a business grade industry standard Cisco device installed in 2009. The firewall is appropriately connected to battery backups to help ensure stability and longevity of hardware. The device provides VPN functionality to the company for external access to the system.

Action - It is recommended the memory be increased and the firmware updated to the most current, stable, and secure version.

Alternative Action – It is recommended that a cloud managed network security appliance be installed to replace the Cisco device eliminating the need for Cisco experienced technicians to make changes and troubleshoot. A new device would also be better suited to handle the increased load from growth in user count since the implementation of the Cisco device.

Action - It is also recommended that a penetration test be run on the firewall to confirm it is, in fact secured appropriately and in line with [COMPANY] expectations.

Internet - GREEN

Locally supported Fiber is in place and bandwidth can be increased by contract. The speed test performed onsite tested within contracted limits. Phones were not reviewed, but the upload speed may need to be increased as performance dictates to accommodate the VOIP phone system and its bandwidth requirements. There is no current need or desire for a failover Internet connection.

> Action – no immediate action necessary. Speed may need to be increased in the future based on needs and/or Internet access behavior changes.

Workstations - YELLOW

There are no XP workstations present that would have had to be mitigated before the end of support in 2014. [COMPANY] is in better shape than most in not having to account for and XP migration plan. There is a mix of Apple and Windows workstations. Windows workstation patching is managed by the local server. Workstations are only able to report to the server while on the internal network.

Action - It is recommended that a cloud based patch management system be implemented to account for laptops when they are not in the office as well as remote users.

Action - To the extent that it's feasible for hardware and software, it is recommended that the operating systems supported be minimized to reduce support costs.

A domain environment is currently configured to manage workstations, security, and accounts. There is discussion of implementing Open Directory for the Mac users.

Action - It is recommended that BRI be Consulted on options and goals to achieve the desired results.

Server/NAS - RED

There are currently 2 physical Windows servers, 1 NAS, and a Mac mini in use. Sapphire is out of warranty. It is a peer of the server Ruby in Active Directory terms.

> Action - It is recommended that the server Sapphire be put on a warranty support contract. Any hardware failure could mean serious downtime and lack of data availability or even loss of data.

Ruby does not have any hardware RAID in place.

> Action – Implement hard drive redundancy on Ruby as a single hard drive failure would bring down the whole server.

The Mac mini does not have any kind of built in redundancy and has no upgrade path.

> Action – Migrate functionality to redundant solution to decrease risk of failure and increase performance.

Open DNS is being used as a forwarder and possibly content filtering.

> Action - It is recommended that the ISP is set as the DNS forwarder and content filtering be managed through a centrally managed cloud based solution.

There are external DNS zones being hosted internally. This means that the internal DNS is overriding public DNS settings has to be manually configured and managed.

> Action - It is recommended that BRI audit and aid in the removal of internally hosted public DNS zones.

Sapphire is currently low on disk space. A Synology NAS has been procured and file share data is in transition to it. BRI has had limited experience with Synology.

> Action - It is recommended that the NAS support model be tested and support contracts be confirmed before all data is migrated to the device.

Email - GREEN

Email is hosted in the cloud with Google Apps. This is a well-known provider. Of note, Google has had some major outages and does not as optimally work with Microsoft Office as a hosted Exchange solution. [COMPANY] did not communicate a need for mail archiving or discovery.

Action – no action necessary.

Optional Action – migrate to hosted Exchange with no migration fees to increase security and uptime.

Optional Action – implement mail archiving policies and solution to protect against accidental or intentional mail deletion and protect against legal issues.

AntiVirus - YELLOW

Kaspersky is managed through the local server. BRI has seen Kaspersky's effectiveness wane in recent years. The licensing model can also be difficult to keep track of. Management and reporting of AV policies are only effective while machines are on the local network. AV can be turned off or even uninstalled while outside the internal [COMPANY] network.

Action - Migrate to a more effective cloud based antivirus solution to keep up with remote users and laptop users when not on the local network.

Licensing - YELLOW

There is no current system in place to track or monitor what applications are installed on the network. The current repository or list of software licensing is not up to date.

Action - It is recommended to implement a cloud based workstation management solution with asset tracking capability and to perform a licensing audit to confirm licensing obligations are met.

Action – Generate a single document or location to track all licensing information such as license keys, costs, and dates.

Physical Environment - YELLOW

There is a sink in one network closet and inadequate HVAC in both. At least one network closet can be accessed by non-IT staff for cleaning purposes. There is no temperature monitoring and alerting in place. A heavy duty chain holds double doors for one network closet together. Access to each closet needs to be restricted and monitored.

Action - It is recommended that appropriate air cooling be installed as well as necessary water damage protection to keep systems up and running. Devices in place without proper air handling may prematurely fail.

Action – Identify if non-IT staff truly require access to closet and if so, install locking network rack to properly secure systems.

Action - It is recommended that a more permanent locking solution be implemented to replace the heavy duty chain to further secure access to IT systems.

Action – Install webcams to monitor and record access to network and server closets to increase security and prevention if webcam is visible.

Policies and Procedures - RED

Device inventory is manually kept and updated. A password policy is in place on the domain. There is an employee departure procedure in place. Given the IT Director's departure, it is recommended that this document be reviewed and updated to consider high level departures with total system access. There is also no standard Employee Onboarding procedure on file. There is no device lifecycle policy in place. Generically a 5 year lifecycle is recommended for infrastructure devices and in some cases 3-5 year lifecycles for end user devices due to the rate of change.

Action – Generate best practices policies and documentation as noted and customize for [COMPANY] to standardize and minimize IT and business risk.

ACTION PLAN SUMMARY

Area	Flag	Action	Associated Hardware/Labor	Associated Costs	Time Frame
Backups	RED	Audit backup configuration.	Estimated 3-4 Hours BRI IT Services Labor	$375-500	Immediate
		Investigate local backup.	Estimated 1-2 Hours BRI IT Services Labor	$125-250	Recommended
		Confirm support model.	Estimated 1-2 Hours BRI IT Services Labor	$125-250	Immediate
		Test and confirm restore data.	Estimated 1-2 Hours BRI IT Services Labor	$125-250	Immediate and Ongoing
Policies and Procedures	RED	Generate best practices policies and documentation.	Estimated 2-3 Hours BRI IT Services Labor per policy/document.	$250-375	Immediate and Ongoing
Firewall/Router	RED	Increase firewall memory and upgrade firmware.	Estimated Memory Hardware Estimated 1-2 Hours BRI IT Services Labor	$100 $125-250	Immediate
		Implement cloud managed firewall.	Estimated Device Hardware and Licensing Estimated 3-4 Hours BRI IT Services Labor	$2000 $375-$500	Immediate Alternative
		Perform penetration test.	Estimated 2-4 Hours BRI IT Services Labor	$250-500	Immediate
Server/NAS	RED	Renew Sapphire warranty.	Warranty Renewal	$150-1500	Immediate
		Migrate all file share data to NAS	Estimated 2-6 Hours BRI IT Services Labor	$250-750	Immediate
		Implement hard drive redundancy.	Estimate Pending Deeper Investigation		Immediate
Server/NAS cont.	RED	Migrate Mac mini functionality to a stable solution.	Estimate Pending Deeper Investigation		Immediate
		Implement cloud	Estimated 2-4	$250-500	3-6 Months

		managed content filtering solution.	Hours BRI IT Services Labor		
		Eliminate external DNS zones from internal DNS.	Estimated 2-8 Hours BRI IT Services Labor	$250-1000	3-6 Months
		Confirm support model and emergency response times.	Estimated 1-2 Hours BRI IT Services Labor	$125-250	Immediate
Physical Environment	YELLOW	Install proper HVAC.	HVAC/Building Contractor		3-6 Months
		Determine closet access and procure lockable hardware.	Estimated Locking Rack Hardware Estimated 2-4 Hours BRI IT Services Labor	$1000 $250-500	3-6 Months
		Install permanent locking solution for main IT closet.	Building/Contractor		3-6 Months
		Install webcams to monitor IT closets.	Estimated 2-6 Hours BRI IT Services Labor	$250-750	3-6 Months
Licensing	YELLOW	Implement cloud based asset tracking.	Estimated 2-6 Hours BRI IT Services Labor Cloud Care for Workstations	$250-750 $4/workstation/month (recurring)	3-6 Months
		Generate document and/or shared tracking workspace.	Estimated 2-4 Hours BRI IT Services Labor	$250-500	3-6 Months
AntiVirus	YELLOW	Migrate to cloud based solution.	Estimated 2-6 Hours BRI IT Services Labor Cloud Care for Workstations	$250-750 $4/workstation/month (recurring)	3-6 Months