



IT Infrastructure & Risk Evaluation

Small Business Self-Assessment Workbook

Overview

This IT Infrastructure and Risk Evaluation Self-Assessment Worksheet is designed to allow small business leaders and decision makers to quickly gain a high-level overview of their IT infrastructure and identify risks or inefficiencies to be addressed.

The evaluation includes 12 critical IT areas grouped into four categories: Security, Communications, Data Protection & Recovery, and Infrastructure.

Each area—such as Anti-Virus software, data backups or remote access—consists of an informational section and a self-assessment. The informational section begins with a concise presentation of the function and value of the technology—i.e. what Anti-Virus software does and why it's important to your business. Then we outline the most common problems we encounter in an area, explain the best practices for your business, and recommend specific technology we consider best-of-class.

Our recommendations are made with no special vendor relationships or benefit to ourselves. We work with a lot of technology and are happy to pass along recommendations for the best small business technologies.

Each area also includes a brief self-assessment that asks specific diagnostic questions. Nearly all are simple enough to be answered by a non-technical person. Those that are not can quickly be answered by your IT resource. These questions help identify any potential problem areas in your business technology, help you assess the level of risk this may present, and design an appropriate response.

About Highland Solutions

Highland Solutions is a Chicago-based firm focused on identifying and solving business issues using technology as a tool. We believe in technology that serves business strategy. Our solutions include IT Support, Managed IT Services, Web Design and Development, Web Hosting and Software as a Service (hosted email, CRM and more).

Table of Contents

SECURITY	4
1: Malware and Anti-Virus Protection	4
2: Firewall	6
3: Content Filtering	8
COMMUNICATIONS	10
4: Physical Network	10
5: Internet Connection	13
6: Email & Collaboration	15
7: Wireless Network	17
DATA PROTECTION & RECOVERY	20
8: Backups	20
9: Data Repositories	23
INFRASTRUCTURE	26
10: PCs	26
11: Printers	29
12: Remote Access	31

Security

1: Malware and Anti-Virus Protection

Function & Value

Malware and Anti-Virus Protection is software that monitors individual PCs for viruses and other malicious programs that may attempt to invade or infect your network. This type of software regularly updates itself with the most recent information about viruses and malware. If it detects an intrusion, it responds by destroying or quarantining the virus, stopping it from infecting the PC or spreading to other computers.

Malware and Anti-Virus Protection functions like a security firm for your house. Its value is in preventing costly damage and disruption.

Common Problems

(1) The use of Anti-Virus software bundled with the PC at purchase. This software must be managed individually on each PC, and typically expires (and stops working) after a year. To maintain protection, varied expiration dates must be recorded and managed. Maintaining the software and the licenses is time consuming and likely to fail.

(2) Failure to provide content protection for Internet browsing. Most viruses and malware now come from websites, not email. Email is typically scanned, but website content is often left unrestricted. Note that content protection is not the same as content filtering. Businesses can protect themselves without restricting employee web access.

Best Practices

(1) Use centralized Malware and Anti-Virus Protection software designed for business networks. These programs run from one “master” computer that provides centralized management and reporting and ensures each PC’s Anti-Virus software is regularly updated. Licenses must be renewed each year, but the software continues to work even after license expiration so your network does not become vulnerable.

(2) Use a firewall with Internet Content Protection to scan and intercept malicious information flowing from the Internet to user’s browsers.

We Recommend

Semantic Endpoint Protection for Anti-Virus Protection
Sonicwall Total Protect Firewall for Internet Content Protection

Malware and Anti-Virus Protection Self-Assessment

Anti-Virus software in use: _____

Is Anti-Virus software on every PC?

Is Anti-Virus software managed centrally?

Does your firewall provide Internet Content Protection?

Level of risk to your business based upon current Anti-Virus Protection:

High

Medium

Low

Issues to be addressed:

- 1.
- 2.
- 3.

2: Firewall

Function & Value

A firewall is the gateway into your network, controlling all inbound and outbound access to and from the servers and PCs you control. A firewall provides the ability to securely access PCs and servers remotely, which is good for telecommuting employees as well as rapid response from your IT firm. Firewalls also often include anti-malware protection, anti-spam abilities (if you host your own email), Internet content filtering and broadcasting for wireless Internet access.

Common Problems

(1) Using a non-business class “all-in-one”. These devices are cheaper, but don’t offer the same tools for remote access and security. They also have limited “throughput”, which means when several people or devices are accessing your server(s) or network at the same time, you get traffic jams.

(2) Failure to secure wireless access. Providing wireless access is great. Providing wireless access to everyone is not as great. Providing wireless access into your private network to everyone is not great at all. It’s bad.

Best Practices

(1) Use a business class firewall. This gives you access not only to solid remote access abilities (both for IT and remote employees), but strong security, anti-malware abilities and content filtering.

(2) Make sure your wireless access is protected. In tech language, “WPA2 Personal” is the safest access protection for a small business. As always, very secure passwords are critical. Many firewalls have the ability to provide both public and private wireless, giving guests internet access and staff full network access.

We Recommend

Sonicwall TZ100 or TZ210 and other business-class firewalls

Firewall Self-Assessment

Firewall in use: _____

Is remote (VPN) access used?

Is Content Filtering used or needed?

Do you provide wireless access?

If so, how is wireless access secured?

Level of risk to your business based upon current Firewall protection:

High

Medium

Low

Issues to be addressed:

- 1.
- 2.
- 3.

3: Content Filtering

Function & Value

A content filter is a piece of hardware or software that acts as a screen between the Internet and your users. The filter uses pre-set and customizable categories to prevent access to types of web sites. The least aggressive filters block only malicious sites, while the most aggressive allow only approved, work-related web sites.

If your organization provides Internet access to minors, you need to know the [legal requirements of Internet content filtering](#).

We advise every organization to use content filtering to block malicious websites. How content filtering is used beyond that depends upon weighing the pros and cons of filtering.

What kind of content filtering is right for your business?

Pros

- (1) Content filtering protects your network from malicious web sites.
- (2) Content filtering can improve productivity by blocking access to personal websites such as Facebook or webmail.
- (3) Content filtering protects the speed of your Internet connection from data intensive uses. We have been asked many times to troubleshoot poor Internet connection speeds where streaming online radio stations were the culprits.

Cons

- (1) Content filtering can block legitimate sites and cause user frustration.
- (2) Content filtering could negatively affect morale. Some organizations allow personal sites to set a tone of trust with their employees. Company culture should be considered when it comes to how aggressively you will filter.
- (3) Content filtering will add administrative overhead, as filters need to be customized to block or allow certain web sites.

Best Practices

Content filtering can be accomplished by a firewall with content filtering software, or by a DNS service. A firewall filter resides at your location, while a DNS filter is a web-based service. Both means use pre-set category templates for you to quickly set how aggressively you wish to filter, and both can be customized with the use of whitelists (sites to allow) and blacklists (sites to block).

We Recommend

Firewall filtering: Sonicwall TZ190 and other business-class firewalls
DNS filtering: OpenDNS for small and medium business

Content Filtering Self-Assessment

Content filter in use: _____

Benefits to your business from using a filter?

Negatives to your business from using a filter?

Types of web sites your business should be filtering:

- 1.
- 2.
- 3.

Communications

4: Physical Network

Function & Value

A physical network is the circulatory system of your technology infrastructure. Switches and Ethernet cables help information circulate between users, servers, databases, and applications. Poorly configured switches and cables can cause your network to run slowly or lose connections.

The physical network is often overlooked in IT evaluations, in favor of “cooler” technology than cables, switches and wall jacks. But if the physical network isn’t rock solid, you’ll see recurring problems over and over again, as wall jacks fail to work, connections are dropped and speed suffers. Poor configuration can also lead to a network looping back on itself, bringing your entire infrastructure to a screeching halt.

Common Problems

(1) Using only a wireless network. Many small businesses begin with a wireless-only network. Wireless is inexpensive and flexible, but it is also less reliable, has slower speed, and is exposed to security risks. Wireless network cards aren’t standard on most desktops, so expanding a wireless-only network can be a hassle.

(2) Poor switch configuration. If you have multiple switches, avoid “daisy-chaining” switches together. A daisy chain is a line of devices, each connected to the one in front of it. This can create multiple “hops” for data to travel through your network. If a PC is connected to the fourth switch in a chain, data coming to that PC would have to take 5 hops (through all 4 switches and then to the PC). Every piece of hardware in the chain has to go to work each time data moves, creating tons of excess traffic.

(3) Insufficient cabling. Wall jacks for Ethernet cables are far too often connected to nothing. A user plugs in and...zip.

(4) Servers and switches in the “danger zone”. Critical network equipment is often stored right out in the middle of the office. People regularly walk by, each one with the potential to bump the equipment and jiggle a cable or power cord lose. Critical equipment set on or under a desk where people can stop to talk and set down their drinks? Yes, it happens.

Best Practices

(1) Investing in a wired, physical network is almost always a worthy capital expense. Make your cables as short as possible. If you have a really big space, 100 meters is the maximum a cable should ever run.

(2) The best practice when setting up a multi-switch environment is to designate one switch as a core switch and to connect other switches to the core switch in a hub-and-spoke layout. Endpoints such as PCs, servers, printers, etc. can be connected to the core switch or secondary switches. This guarantees there are no more than two hops between any two switches and no more than four hops between any two devices.

(3) If you have more wall jacks than users, wire all the jacks and connect them to switches. Purchase switches based on your number of wall jacks. This allows you to grow into your network, and avoid juggling jacks on your switch.

(4) Designate a closet or out-of-the-way place as a space for your network equipment, including server, switches, firewall, etc. A wall mount rack is a small investment that will help secure, organize and safeguard your valuable equipment.

Physical Network Self-Assessment

Is your primary network wired or wireless?

Are switches configured correctly?

Is every wall jack active?

Are cables the correct length and properly organized?

Is your server in a “danger zone”?

Issues to be addressed:

- 1.
- 2.
- 3.

5: Internet Connection

Function & Value

Your Internet connection...connects you to the Internet. Depending on your business, this is either a nice benefit or life and death. How critical web access is to your business will determine how much attention and budget you give to Internet connectivity.

Common Problems

(1) Using an underpowered connection. DSL connections are nearly always over-rated. This means if your provider claims the connection is—for example—1.5 Mbps (megabytes per second) down and .2 Mbps up, the speed you actually experience will be less. We suspect published DSL speeds can only be experienced under better-than-ideal conditions.

(2) Relying on a single connection for an Internet-dependent business. If online access is necessary for your business or your staff to function, a single connection will cause downtime. The cost of downtime (in productivity, customer relations and recovery) will probably cost much more than a backup connection.

Best Practices

(1) Consider a T1 instead of DSL. A T1 line is a fiber optic connection that is considerably faster than DSL. You can test your Internet speed online at <http://www.speedtest.net>.

T1 agreements are more expensive. But in addition to better speed, T1 agreements usually have better Service Level Agreements than DSL lines. So not only is the line faster, but your provider will promise to resolve issues more quickly.

(2) If you need to ensure Internet connectivity, use redundant circuits. This means ordering T1 or DSL lines from different cabling plants. Different providers are usually using different cables, but ask your secondary provider to be sure. Your firewall can be configured with a primary and secondary connection and can route overflow traffic to the secondary line, or sense when the primary line is down and switch all traffic over. The end result is fairly seamless and makes it much less likely for your office to be disconnected.

Internet Connection Self-Assessment

What kind of Internet connection do you currently use?

Current speed? (<http://www.speedtest.net>)

What abilities does your business lose when disconnected from the Internet?

How critical is constant connectivity to your business?

High

Medium

Low

Issues to be addressed:

- 1.
- 2.
- 3.

6: Email & Collaboration

Function & Value

Email has become **the** central form of communication for business. Email is critical to your company in marketing, sales, customer service, operations and more.

A host of related functions have grown up around email: calendars, contact lists, task lists, instant messaging, etc. Collaboration technology takes these functions and connects them: you see not only your own calendar, but also your team members'. Contact lists, project tasks and more now become shared information. The effects on productivity are incredible.

Common Problems

(1) Lack of collaboration. Email is provided (often for free) by a website host, and is accessed through a basic webmail program or Outlook. This creates two major issues:

- Each employee's information is on an "island", with no ability to share schedules, contact information, or to-do lists. *This is a massive time sink with significant cost to your business.*
- All email and related information is stored on individual PCs. When a hard drive fails, all of that information is lost. *This is a massive business risk with significant potential cost to your business.*

Take an informal survey. Find out how much time staff is spending each week managing contacts and calendars, or making phone calls and emails to set up meetings. Multiply that out into annual salary to see what lack of collaboration is costing your business. (And that's not even considering lost revenue from all that wasted time!)

(2) Overly complex and costly tools. The collaboration tools with the most brand recognition (Microsoft Exchange, Novell Groupwise, Lotus Notes) were made for very large corporations. They work in economies of scale. 1,000 users utilizing a \$10,000 investment makes a lot of sense. 25 users utilizing a \$10,000 investment does not. These tools are too costly and complex to maintain for smaller businesses.

Best Practices

(1) Use collaboration tools. Your staff will thank you, and your general ledger will too. There is no other piece of general software that will have more impact on your staff's productivity.

(2) Use a hosting provider to deliver the software as a service. Web based collaboration systems are the best solutions for small and medium size businesses. Zimbra Collaboration Suite is the current best-of-breed hosted solution. If you're a Microsoft-only shop, you can get Exchange as a hosted solution through a provider.

Email & Collaboration Self-Assessment

Email provider: _____

Do you currently use collaboration tools?

Estimated annual staff hours spent on collaborative tasks (updating contacts, scheduling meetings, coordinating tasks): _____

Where is email and related information stored? Is it backed up?

Total cost of current solution: _____ per year

(If currently using Microsoft Exchange, see the Exchange Total Cost of Ownership calculator below.)

Issues to be addressed:

- 1.
- 2.
- 3.



7: Wireless Network

Function & Value

A wireless network allows wireless enabled devices like laptops and PDAs to easily gain access to the Internet or your local network.

Why do you need a wireless network?

Wireless is more flexible and less expensive than a wired network and can be ideal for small or mobile offices as a primary network. Wireless also makes your office hospitable to guests needing access.

Why don't you need a wireless network?

Unlike wired networks, you cannot control how far a wireless network extends, so your network can be accessible from the parking lot or the office next door. Wireless is also much more difficult to secure than a wired network, and poses unique security challenges.

Wireless isn't right for all businesses. If you already have a wired network, don't add a wireless network unless there is real need.

If you do have or require a wireless network, pay attention to the following common problems and best practices. A compromise of your wireless network can be crippling to your business.

Common Problems

(1) Unsecure networks. Many wireless networks are incredibly easy to compromise. If you're still using the factory default settings for security and admin credentials, you're at high risk.

(2) No distinction between guest and internal networks. Guests need Internet access without an open door into your file server.

(3) High interference and poor performance. Wireless routers broadcast on channels. If a neighbor's wireless network is using the same or similar channel, it can negatively impact the speed of your network.

(4) Weak signals. Placement of your wireless router determines what areas of your office can connect reliably to the network. Poorly planned wireless networks can have dead and weak spots.

Best Practices

(1) Change the default configurations in your wireless router. A simple Internet search can yield the default IP address, user name and password for every wireless router ever made. If you don't change the defaults, anyone over the age of 10 could break into your network.

(2) Turn the security settings on. Security on wireless routers is usually off by default. There are three types of wireless security. From best to worst they are:

- WPA2
- WPA
- WEP

If you're serious about security, use WPA2. If you don't have it, use WPA with a strong key. Your key should be random or at least non-dictionary standard, like "iwantmywireless2bsecure". WEP is not recommended, but if it is the only option available, change the default key from the factory. You should involve an IT professional to configure your security correctly.

(3) If you intend to offer wireless for staff and guests, use two wireless networks. Put Internet access, and perhaps access to a printer, on your guest wireless. If you need full network wireless access, place it on a separate wireless network with very strong security. Turn broadcasting off for an internal network, as guests (or the office next door) don't need to discover it.

(4) Change the default channel. Wireless routers have 11 channels, with channel 6 as the default. Only channels 1, 6 and 11 do not overlap. Some routers can scan and find uncontested space, as can free tools like NetStumbler and Kismet.

(5) Perform a site survey. There are very good (and very expensive) tools to generate an accurate site survey of your wireless network. NetStumbler or Kismet can help you perform a rough site survey as well.

(6) Don't use really cheap equipment. You'll pay in productivity. Cheap wireless routers are cheap for a reason. A few extra hundred dollars up front will pay off in the long run.

Wireless Network Self-Assessment

Are you currently using a wireless network?

What purpose does/would a wireless network serve in your business?

Have you changed the wireless router defaults?

What security does your wireless network use?

Can wireless guests access your internal network?

Level of risk to your business based upon current wireless:

High

Medium

Low

Issues to be addressed:

- 1.
- 2.
- 3.

Data Protection & Recovery

8: Backups

Function & Value

Backups create copies of critical business information. Computer hard drives fail, laptops are stolen, buildings catch on fire, data is accidentally (or intentionally deleted). Backups ensure these events don't permanently destroy data.

Backups are not very interesting, and tend to be neglected. They're hard to care about when nothing has gone wrong for years at a time. But in times of unexpected disaster, an accessible backup can save days, weeks or years of work. A backup can even determine if a business survives or closes its doors.

Here are six killer backup mistakes.

Common Problems

- (1) Data is not centralized. Most small businesses run one backup: the file server. If your staff isn't disciplined in saving their work onto the file server, your backup will be incomplete. And since the documents your staff worked on recently are typically the most important ones, what you'll be missing is likely what you'll most need.
- (2) Backups are not reported. If email alerts aren't sent out when a backup completes or fails, backups are out of mind. If your backup failed for the last two months, would you know?
- (3) Over-reliance on manual processes. The more things a person has to remember to do, the less reliable your backups will be. Manually copying files to an external drive or a CD is not a backup process, it's a recipe for disaster.
- (4) Backup data is not off site. Backing up to a second hard drive or a backup tape in the closet will save you from drive failure, but it won't help in case of disaster or loss of access to your building. Many risks still remain when backup data is in the same physical location.
- (5) No thought is given to how to restore data. Backup strategy often ends with moving the data offsite. But what happens when you need to restore that data quickly? Can you read your tape drive? Will you need to install specific software to use the data?
- (6) Financials are not treated differently. Financial data must be current and easily retrievable. Lumping it in with large, weekly backups is a mistake.

Best Practices

(1) Use your server. Make clear server use policies and enforce them. No critical data should ever be stored solely on a local PC. Consider configuring your network with roaming profiles, or to automatically store My Documents folders on the server.

(2) Configure your backup to send a status email no matter what, each time a backup is performed.

(3) Automate backups every night using dedicated backup software such as Retrospect.

(4) Take data off site. Better yet, consider online backups such as Mozy. Like most online solutions, there are no up front costs, but there are recurring monthly fees. At \$0.50 per GB per month, it's very cost effective for most businesses, and eliminates any worry about getting backups offsite.

Be aware of bandwidth limits and fees from your provider, in case online backups would cause you to incur bandwidth fees as well.

(5) Don't use tape drives. If online backups aren't right for you, use an external hard drive system.

(6) Backup financials online every day. Many accounting software providers, such as Intuit with Quickbooks, offer daily online backup features. Annual fees are minimal to ensure your financials are current and easily retrievable in case of a crisis. You (or your accountant) will need access to off-site copies of your accounting software as part of your disaster recovery planning.

We Recommend

MozyPro Online Backup

Backups Self-Assessment

Backup software in use:

Devices backed up and schedule (daily, weekly, etc.):

- 1.
- 2.
- 3.

Devices not backed up:

What part of your backup plan is not automated?

Is backup data off site?

How will backup data be restored?

How is financial data backed up and on what schedule?

Level of risk to your business based upon current backups:

High	Medium	Low
------	--------	-----

Issues to be addressed:

- 1.
- 2.
- 3.



9: Data Repositories

Function & Value

Data repositories keep your critical business information centralized and secure. For most small businesses, the sole or primary repository is a file server. Other common data repositories are hosted file management systems, industry specific applications, and customer relationship management databases.

A centralized server makes files accessible and organized, and protects your business from loss due to employee turnover or computer failure.

A server is often one of the first IT purchases for a new business, but many are underutilized, insecure or improperly configured. This leads to continued exposure to risk, both internal and external. Here are the most common problems small businesses encounter with a file server and how to avoid them.

Common Problems

(1) Not owning or using a server, or a web based file management system. We've seen networked PCs with no server and servers sitting in the corner. A converted PC is a poor substitute for a real file server (see #4 below).

(2) Lack of storage policies. A file server is only useful if it is used. If a server contains documents from 2 years ago, but the huge proposal or job in progress is in My Documents on a PC somewhere, the server isn't serving your business.

(3) No security restrictions on access. Your HR and financial files benefit from the security of a file server, but they shouldn't be visible to every employee who can access the server.

(4) A single point of failure. A server should protect your data by storing multiple copies, along with daily backups. A server with a single hard drive has a single point of failure. When that hard drive goes, *everything* could go with it.

Best Practices

(1) Use a real server. Enough said.

(2) Store everything on the server. Make sure your staff knows every document of value gets stored there. Every day. No exceptions. Alternatively, you can create profiles on your local server, with the My Documents on every machine actually storing to the server itself and not the local hard drive.

(3) Create root folders on the server for sensitive information, such as HR and accounting. Restrict access so only those with a need to know can view those folders.

(4) Use a RAID configuration on your server to ensure your data will not be lost. RAID enables a server to maintain mirror copies of your data on multiple hard drives.

We Recommend

HP Servers

Linux file servers, for higher reliability and security at a lower cost



Highland Solutions

Data Repositories Self-Assessment

Server in use:

How much of your data do you estimate is stored on the server?

Do you have storage policies in place?

Do My Documents folders store on the server?

Is any sensitive information visible to all of your staff?

Does your server have a RAID configuration?

Level of risk to your business based upon current server configuration:

High Medium Low

Issues to be addressed:

- 1.
- 2.
- 3.

Infrastructure

10: PCs

Function & Value

The personal computer is everywhere. For most businesses, it is as essential as a phone and a business card. Maybe more so. PCs enable, connect, and extend. PCs serve as a platform for nearly everything a knowledge worker does.

These days, PCs are cheap. But maintaining them is not. Neither is a lost day of work when one breaks. Here are the most common problems that lead to expensive maintenance and lost work, and how to ensure your PCs are reliable.

Common Problems

(1) Non-standardized operating systems. If you are the do-it-yourself type, or your IT person is, you'll have a mishmash of PCs and Windows versions throughout your office. It seems like you are saving money by using available resources so well. But chances are, you're not. A mishmash of PCs means added confusion when troubleshooting, more things that can break, and a host of networking problems. On office networks, any Home version of Microsoft Windows causes problems. Home's networking capabilities are limited.

(2) Aging machines. PCs have a life span of three to five years. A PC may still be powerful enough to do what you need, but the chances of hardware failure increase greatly after a few years.

(3) Too much time and cost spent on maintenance. The cost of purchasing a PC is much less than the cost of keeping a limping PC going. In general, the purchase cost of a PC is only 20% of what that machine will cost your business over its lifespan. Non-standardize and old machines are time and money pits.

(4) No centralized management and access control. If user accounts and file stores are scattered across the PCs in your office, your options are limited when passwords are lost or employees leave. It can be difficult to regain access to a machine or the data on that machine. If an employee or ex-employee uses encryption on their data store, information could be lost forever.

Best Practices

(1) Standardize operating systems. Always use professional versions, and, as much as possible, make them all the same. For most businesses right now, that means XP Pro, with Windows 7 as the next upgrade. Vista should be avoided. Working on a single platform provides a constant variable in supporting and maintaining your machines. Since IT won't have to track down problems with three or more operating systems, you'll save money.

(2) Have an Evergreen policy and budget. Evergreen policies schedule PC replacement over a three to five year cycle, replacing 1/3 to 1/5 of your PCs every year. Staggering upgrades every year ensures you don't end up with ancient, ailing machines and have to face a costly, full-scale replacement.

(3) Use an image for similar PCs. A PC image is an operating system, settings and common applications bundled together into a disk image that can be quickly applied to any PC. When a PC has problems, have IT re-image the PC and start over fresh. This takes 60 minutes, as opposed to spending an unknown number of hours trying to find and resolve the issue. If your staff is storing all data on the file server, no data should be lost during a re-image.

(4) Use domain logons, not PC logons. Domain logons give you centralized profile management and access control, so PC access and data storage is always under your control.

PC Self-Assessment

Number of PCs:

Operating system(s) in use:

Average age of PCs:

Is an Evergreen policy and budget in place?

Is a PC image used?

Are domain logons in use?

Level of risk to your business based upon current PC use:

High Medium Low

Issues to be addressed:

- 1.
- 2.
- 3.

11: Printers

Print easily and as cheaply as possible. That's the bottom line with printers. Here are the three most common mistakes businesses make with printers, and how to fix them.

Common Problems

(1) Sharing printers off of PCs. When a printer is connected directly to a PC and then shared through the PC, it slows down printing and can affect the shared PC's performance. Anytime the PC is turned off, the printer is unavailable.

(2) Sharing printers off of a server. This creates similar problems and is unnecessary. Current printers have the processing power built in to handle virtually any print job you can send their way. There are some situations where sharing off of a print server is advantageous (see below).

(3) Using inkjet printers. To some extent, all printers are "cheap" and all ink is "expensive", but inkjet printers are the worst of the lot. The low purchase price of the printer disguises the fact that over time inkjets are more expensive than laser printers. Similarly, printing black and white documents to a color printer wastes more expensive ink consumables.

Best Practices

(1) Share printers directly on the network. Network enabled printers usually have a "n" at the end of their model number. These printers have Ethernet jacks and network cards built in, and are available on your entire office network for PCs to print to.

(2) Use direct IP printing instead of a print server. Again, simpler is better. There are exceptions to this rule. If you need quick printing for guests to your office, or if remote employees need to print on the office printer, leave a printer on the server.

(3) Buy a solid monochrome laser printer for the majority of your printing. Internal drafts and black and white documents should always go to this printer. You can set grayscale and duplex on by default to save even more ink and paper. By all means, print your final versions with color ink and nice paper, but there's no need to waste expensive consumables on drafts and memos.

Printers Self-Assessment

Number of printers in office:

Types of printers (inkjet, color, laser)?

Are any printers shared from a PC?

Are any printers shared from a server?

What is the estimated cost per page for the ink replacements for your printers?

Which of your printers has the cheapest consumables?

Issues to be addressed:

- 1.
- 2.
- 3.

12: Remote Access

Function & Value

Remote access enables users to access programs and files stored on a PC or server in your office when they are not physically in the office. Remote access can allow for a flexible work schedule, cover mistakes when a file or task is forgotten, and help you accomplish an emergency weekend task without an emergency weekend commute.

There are two common ways to provide remote access: VPN (virtual private network) and Remote Desktop. A VPN uses a piece of software on an external PC to connect with a VPN concentrator (often a firewall) inside the office. Remote Desktop runs on an external PC and connects with appropriate credentials to a PC inside the office.

External access is required for most businesses, but it can pose significant risks to your network. Here are the most common problems and how to avoid them:

Common Problems

(1) Granting too much access. If VPN rights are unrestricted, remote users can gain access to everything on your network.

(2) Lack of end user policies. Your network may be very secure, but what happens when remote employees start pulling files and data down onto their home network? Do you know who is able to connect remotely, and what they are allowed to do?

(3) Using the wrong tools. If there is a strong need for remote access, it may be a sign you need to evaluate the tools you are using. Traditional PC or server bound software is relatively difficult to access remotely, but newer web-based solutions make remote access obsolete.

Best Practices

(1) Give minimal access. When a VPN is configured for remote access, grant the minimum amount of access for a user to accomplish their work. You don't want a score of VPN credentials out there that all have complete access to your entire network.

(2) Have clear end user policies. You can't secure your users' home networks, but you can educate them. What can they bring down and store on a local PC? Is their wireless network broadcasting or unsecure? Set standards for your remote access employees.

(3) When appropriate, use web-based tools. Web-based tools are available for email, databases, document storage, project management and more. The technology is so mature that often there is an increase in functionality when moving off of server-bound applications.

Remote Access Self-Assessment

Type(s) of remote access in use: _____

Is access appropriately limited?

Do employees have clear guidelines for home network security?

Is most remote access driven by a single need? Could a web-based solution remove most remote access?

Level of risk to your business based upon current remote access:

High Medium Low

Issues to be addressed:

- 1.
- 2.
- 3.

Now What?

The Highland Solutions team hopes this do-it-yourself IT assessment guide has helped you isolate key issues and opportunities for your business.

We would welcome the change to assist you in addressing particular issues or opportunities. We can be reached at 312-863-7500 and info@highlandsolutions.com.