The Basics of Securing Your Business

Discover how to:

- ✓ Reduce the risk of security threats
- ✓ Provide safe remote access for employees
- ✓ Enjoy peace of mind with layered security
- ✓ Save time and money with integrated protection

Brought to you by Intega IT | www.intega.ca/it-services/it-security

When it comes to your business, there is nothing as essential - or as vulnerable - as your network. This technology provides access to your critical applications and houses your business data. And yet, while securing your business data and systems is a basic responsibility, it can be a complex challenge.

Whether it is hackers, property theft, employee safety, the loss of customer data or employees using company information while away from the office—there is a lot to think about.

This guide can help to relieve your worries about your potential risk exposure with simple and cost effective ways to protect your business assets while providing appropriate access to information.

Did you know a single network security breach can shut down your operation for days or even allow a hacker to steal vital business data? That's why it's important to secure your network against these common threats:

E-mails and Website visits that can introduce viruses, spyware, and malware.
These programs can install themselves on your computers and record passwords or troll through files for credit card, bank account and other sensitive information.

Human intruders who can steal sensitive information about your company or customers.
The number of organizations targeted by professional attackers is likely to grow. While much of the current professional cybercrime activity targets home users, organizations will likely see more infected systems attempting to access protected networks.

Never assume network attacks will only come from outsiders. Loyal employees can inadvertently create security vulnerabilities. And disgruntled or former employees can cause considerable damage if they have access to secure information.

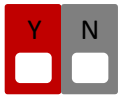
WHO: Your Power People

Before you delve into security technologies, consider who will be using them and how to lead a successful program.

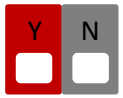
- Favor technologies that are fast and easy for employees and partners to use—so they will use them.
- Create a written network security policy that defines the types of network use that are required, allowed and prohibited. Model it yourself. The policy should be concise, clear, kept current, and enforced.
- Educate employees on security risks and train them on your policy, informally as needed and more formally at least annually. Use security problems that arise as opportunities to learn and increase awareness.
- Reward employees who exemplify smart security behavior.

Where Do You Need Security?

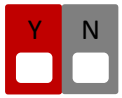
In order to quickly identify potential risks and gaps in the security of your business network, answer these five questions:



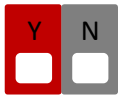
Does your business have enough protection against Internet threats? We have been accustomed to thinking about online threats only as viruses. The reality is that the most likely threats are malware: bots, spyware, worms, rootkits and Trojan horses. In order to combat these threats, it is important to do more than just running anti-virus software on individual computers.



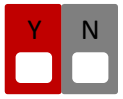
Do you safeguard your critical business data? Do you have a specific methods for storing and backing up information from laptops, PCs, servers, smartphones and USB sticks? Are you storing this information in more than one place?



Is the internal business information readily available? Can employees access this information wherever they are to do their jobs? Do you have control over who can access specific types of information and from where?



Does your business have video surveillance? Are you able to monitor your business and employees?



When visitors connect to your network do you control their access? Are you sure that your wireless network is not available to others?

Any question you answered no to, this is where your business should be focusing attention for security.

How a Business Does It: The Security Trifecta

The key to network security is found in a simple model: confidentiality, integrity and availability (CIA).

It is important to remember that no single technology can meet all your security needs. This is why multiple layers of security are needed—from hardware to software—and require regular updates and reviews to protect against new threats.

Confidentiality

Your private business information should be kept away from individuals who should not have access.

Technologies that can help with ensuring confidentiality include:

- Identity management
- Firewall
- VPNs
- Virtual LAN (VLAN)

Integrity

Data available on your business network and devices should not be lost or altered.

Technologies for protecting the integrity of your data include:

- Secure storage
- Data encryption
- Virus scanning
- Web security software

Availability

Employees, customers and business partners should have reliable and timely access to the resources they are authorized to use.

Technologies for protecting the availability of data include:

- Video surveillance
- Intrusion prevention system (IPS)
- Spam filtering
- Secure wireless network

We're ready to help. Intega IT can help protect your business with affordable layered security hardware and software solutions that fit your unique business needs.

To learn more about IT Security and how these processes can benefit your business, please contact Intega IT at (613)260-1114 or by email at sales@intega.ca.

What You Can Do Now to Protect Your Business

Now that you have learned the basics of network security, here are some tips to help you decide which technologies you need:

- Identify the value of the assets in your business (their impact on operations costs and sales, as well as their replacement cost).
- For each high-value asset, assess its CIA vulnerabilities. Now you can prioritize the protection that your business needs most.
- Inventory the security capabilities your business already has, then focus on the gaps.
- Choose solutions that work together; integration improves performance and security, and the productivity of technical staff.