I picked a coffee shop. Every small business conducts various aspects of their business with computer processing. A business generally uses computer software that either:

1) Performs the entire process on the premises (in-house) on one computer (standalone) or

2) Accepts and stores data entry, communicates and transmits the data to an (off-site) server computer, for server-side processing (client-server networking). The Internet is the most common media for business-to-business (B2B) transactions with established trading partners. Further, larger companies have more transactions and may use electronic data interchange (EDI).

Common services needed from other businesses are merchant banking, personnel payroll processing, accounts receivable for credit cards, accounts payable with suppliers and vendors, inventory control for ordering and shipping, and progress reporting requirements for funding.

In addition, a new norm is the smartphone Application (App) that runs software to perform client-server networking, via Internet connectivity through either Wi-Fi or Cell-Data. There are numerous apps that do specific tasks, e.g. tracking, reporting, scheduling. A good example of a secure application for the coffee shop’s staff scheduling is ScheduleFly.[[1]](#footnote-1)

The business may be managed by more than one person and with more than one computer. Each business computer is usually dedicated for their specific task but are also connected together (networked) in a local area network (LAN) for other, general tasks. Most importantly, a business may have a file-server on the LAN that is a central repository for all their business-critical data. A central location, security software/hardware and security policies can safeguard the data with controlled access and consistent data backup/recovery. These layers of security affords three protections: confidentially, integrity, and availability (CIA).[[2]](#footnote-2)

To discover what is typically done, I used the Bing search engine and as I typed, the textbox auto-filled with “small business network security checklist.” The search results are listed by popularity (usually the best are at the top) and I read a few but found the first article, from Cisco, to be very good: “Network Security Checklist”[[3]](#footnote-3) It states, “Many small and medium-sized businesses do not have adequate network security. Here's how to make sure you do” and in brief:

**Network Security Checklist**

Every business should have a written (and thoughtfully prepared) **network security plan** in place. A thorough policy will cover topics such as:

* **Acceptable use policy**, to specify what types of network activities are allowed and prohibited
* **E-mail and communications activities**, to help minimize problems from e-mail attachments
* **Antivirus policy**, to strengthen awareness of threats like viruses, worms, and Trojan horses
* **Identity policy**, to help safeguard the network from unauthorized users
* **Password policy**, to help employees select strong passwords and protect them
* **Encryption policy**, to provide guidance on using encryption technology to protect data
* **Remote access policy**, to help employees safely access the network when outside the office

**Inventory and Acquire Your Security Technologies**

* **Firewall**, to keep unauthorized users off your network
* **Virtual private network (VPN)**, for secure access to your network
* **Intrusion prevention**, to detect and stop threats before they harm your network
* **Content security**, to protect your network from viruses, spam, spyware, and other attacks
* **Secure wireless network**, to provide safe network access to visitors and employees on the go
* **Identity management**, to give you control over who and what can access the network
* **Compliance validation**, to ensure devices accessing the network meet security requirements

**Identify Your Most Important Digital Assets and Who Uses Them**

* Know what are your company's digital assets, i.e. intellectual property and customer records
* Know what they are worth
* Know where those assets reside
* Know who has access to these assets, and why
* If you extend access to business partners and customers, know how you control that access

**What Would a Security Breach Do to Your Business?**

* What is the potential financial impact of a network outage due to a security breach?
* Could a security breach disrupt your supply chain?
* What would happen if your Website went down?
* If you have e-commerce on your site, how long could the site be down before losing money?
* Are you insured against Internet attacks, or against the misuse of your customers' data?
* Do you have backup and recovery capabilities to restore information after a security breach?

**Consider Your Current and Future Needs**

* How do you expect your business plan to evolve over the next few years?
* How recently have you updated your network equipment? Software? Virus definitions?
* What type of security training do you provide to your employees?
* How will growth affect your digital assets and their value to your business as a whole?

About me: In 1997, I was hired as a Network Administrator for the organization of Volunteers of America in San Diego, California. I managed the information security for the Corporate Office and HIPAA for thirteen program facilities, in three counties and over 100 computing personnel.

1. ScheduleFly – a restaurant staff scheduling and communication application. Downloaded from <http://www.schedulefly.com/> [↑](#footnote-ref-1)
2. Security - "Little Black Book" of IT Mgmt. Downloaded from <http://itec711.wikidot.com/security>

   [↑](#footnote-ref-2)
3. Network Security Checklist. Downloaded from <http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/secure_my_business/network_security_checklist/index.html> [↑](#footnote-ref-3)