AOR INFORMATION TECHNOLOGY SOLUTIONS

1058 Clemens Ave, Roslyn PA 19001, 215-219-3786

Cyber Security

What is it?

Dictionary.com defines it as: **precautions taken to guard against crime that involves the Internet, especially unauthorized access to computer systems and data connected to the Internet.**

What can it do to your business.

1. It can wipe out all your data on your computers.
    a. Disruption caused by this.
        i. Accounting not knowing how much cash is in check book
        ii. Not knowing who owes money for sales. (A/R)
    b. All Programs can be destroyed so even if you have the data you cannot get at it.
    c. Any Manufacturing equipment that uses a computer can be compromised and become unusable.
    d. Scheduling and ERP systems cannot function. The manufacturing process will then stop.
    e. Shipping will stop due to most shippers now use computers to create bills of lading and other shipping forms.
2. Your data can be stolen and used for illegal purposes.
    a. Credit card numbers can be stolen.
    b. Bank access logins can be stolen and used.
        i. Customers checking accounts can be stolen.
        ii. Your bank accounts can be emptied.
        iii. Your credit lines can be run up to maximum.
3. Some Numbers
    a. 60% of Companies have been hit by Ransomware
    b. 63% were down for more than a day.
    c. 70% of these companies paid the ransome.
    d. 40% of spam contains Ransomware.

Types of attacks

1. Insider-
    a. This is a disgruntled employee that is holding some type of grudge and has access to the systems. This attack is almost impossible to stop except to fire the person and remove all access for them.
    b. An inside person caught in a Phishing attack addressed to the corporate email.
    c. An insider can hit a dirty web site and bring in an attack such as Malware or Ransomeware.
2. Outsider
    a. This could be an attack on the firewall.
    b. This could be an attack brought in via a company email
    c. This could be an attack brought in via a personal email.
    d. This could be an attack that crawls from one computer to the next. One laptop could get an infection while outside the network and then bring it into the network.
    e. This could be a compromised web site.

Can you stop all attacks?

No. You can only minimize the attacks and minimize the damage.

Conduct Social Engineering Training. This will teach employee's what to look out for so they do not bring in threats such as ransomware.

How do you minimize the effect on the business?

Create a disaster recovery plan.

1. The plan must include a backup strategy
2. The backup plan needs multiple parts.
    a. The servers
    b. The workstations
    c. The laptops
3. It must include a network perimeter strategy
    a. This would include a plan for a firewall with a update subscription.
    b. Also the wifi must be considered.
    c. It must include a server strategy
    d. If you use Virtual servers
        i. separate out the main functions.
        ii. Make a snapshot backup of each server beside each normal backup.
    e. Create a plan for anti-virus.

4. It must include an individual pc strategy
    a. It must include a restore plan.
        i. Does the plan need to restore only the programs or also the data (do you store the data on the server)
        ii. What firewall protection do you need
        iii. What anti-virus protection do you need.
        iv. Is it a Laptop that travels outside the network?

    b. What application lock downs do you need.
        i. There is a big trade off from locking down the PC and allowing users access.
        ii. Do you have the manpower onsite to open applications users might need.
5. It must include a remote user strategy

Note There are different types of anti-virus.

1. Is anti-malware- This is geared toward malware type of infections. (examples Malwarebytes)
2. Is traditional anti-virus. This waits until someone gets a virus and then the company creates a definition to do a pattern match to protect others.
3. Is a proactive anti-virus/anti-malware/anti-ransomware. This program detects suspicious behavior before a virus become known and blocks it. This is the only products that truly stopped the latest Petya Ransomware from the beginning.