COMPUTER SECURITY & DISASTER RECOVERY

Fundamentals for Small Business Managers

You've Got Mail...

Hi,

I hacked your computer.

I got everything you typed (passwords, etc.) for the past few weeks.

I changed the passwords on all your online accounts.

If you want access to your company files, email, website, QuickBooks, etc. send money NOW.

Delay, and I'll tell every customer in your database you lost their information due to pure negligence.

How much will that cost you? You have one hour.

Sincerely,

ATTACKMASTER

The Shocking Truth About Cybercrime

At ($388bn) it is larger than the global black market in marijuana, cocaine and heroin combined ($288bn) and approaching the value of all global drug trafficking ($411bn)

431m adults experienced cybercrime

More than a million become victims every day

14 victims of cybercrime every second

Norton Cybercrime Report 2011

The Shocking Truth About Cybercrime

69% of adults surveyed have experienced cybercrime in their lifetime

3X more victims of cybercrime than offline crime

The odds an consumer will become a victim of cybercrime in a year
1 in 2.27

But 41% admit they do not have up-to-date security software

Norton Cybercrime Report 2011

The Security Disconnect

Safe local communities = false sense of security online

Only 31% think they are more likely to be a victim of cybercrime than a crime in the physical world - e.g. burglary

Reactive mentality

No training, policies, or auditing

No disaster recovery plan

Security Requires Strategy

~~Internet~~

Physical

Gateway

- Modem
- Firewall
- Router
- Wireless

Computers

- Users

10 Steps to Improve Security

Control Physical Access

- Lock up laptops (cable lock, locked room, encryption, Lojack)

- Use a locked room for servers and backups

- Engage unknown guests

- Monitor traffic with cameras

- Monitored alarm system

10 Steps to Improve Security

Add a Gateway Firewall

- Network Address Translation (NAT)

- Statefull Packet Inspection (SPI)

- White List (web filter)

- Change factory default logins

- Disable remote administration

10 Steps to Improve Security

Secure Wireless Networks

- Disable SSID broadcast
- Use WPA2 Personal AES encryption
- Change factory default logins
- Disable wireless administration
- Beware of WiFi travel risks

10 Steps to Improve Security

Use Anti-Virus Software

- Every computer (also home)
- Update frequently (daily)
- Scan frequently (real-time)
- Consider a protection suite
- Symantec Norton Internet Security 2013 / AVG Anti-Virus Free 2013

10 Steps to Improve Security

Install Software Patches / Updates

- Operating System Updates
- Applications
- Printers
- Firmware

10 Steps to Improve Security

Require Individual User Accounts

- One for each employee, passwords required

- No sharing or borrowing

- No administrator accounts

- Enables auditing

- Access control (termination, account theft, data privacy)

10 Steps to Improve Security

Limit User Access to Data and Computers

- NO ADMINISTRATORS   What about office managers?

- Access only job specific systems and data

- No authority to install software

- Minimize file sharing

10 Steps to Improve Security

Regularly Change Passwords

- Every 90 days
- Inevitable sharing, notes, Post-Its, loose lips
- Require strong passwords (letters, numbers, capitalize, phrases)
- Use different passwords for each account
- Password Safe

10 Steps to Improve Security

Regularly Change Passwords

- Every 90 days
- Inevitable sharing, notes, Post-Its, loose lips
- Require strong passwords (letters, numbers, capitalize, phrases)
- Use different passwords for each account
- Password Safe

Wehave24lunch

MyFamilyOf4

IseeU812

10 Steps to Improve Security

Train Employees in Security Principles

- eMail (attachments, privacy)
- Web (white list, downloads, apps, plug-ins, toolbars)
- Phone (login dissemination, environment details)
- Intra-Office (data access restrictions, account sharing, removable media)
- Designate a point of contact for computer security

10 Steps to Improve Security

Backup, Backup, Backup

- The heart of any disaster recovery plan
- Office documents, spreadsheets, databases, financials, email, passwords
- All computers you can't live without
- Store backups on a separate drive (USB, network, online)
- Keep multiple versions
- Password protect or encrypt the backups

* Restoring from a backup is often the only option for system recovery

Your Number Is Up

Planning for Disaster

Disaster Recovery Planning

Natural

- Lightning, tornadoes, floods, wildfires

Common

- Hardware failure
- Vandalism (hacking, malware, virus)
- Accidents (deletion, falls, spills)
- Theft (physical, electronic)
- Sabotage
- Fire, water, smoke damage, power surges

Disaster Recovery Planning

Two Primary Questions

1. How long can the business function without the data or computer system?
2. How long will it take to recreate missing data?

The answers to these two questions determine the recovery strategy.

Proactive preparation is the key to success.

Disaster Recovery Planning

Disaster, Who Cares?

The computer or data is expendable.

Plan to celebrate its short life and move on...

Disaster Recovery Planning

Disaster, How Annoying!

The computer can be replaced or the data can be recreated in a short amount of time.

- Weekly backups of the most important items
- Transfer a backup to an off site location at least once a month.
- Automate the backup process

- Backup software
  (Windows Backup, Livedrive, Mosy, Carbonite, Symantec)
- Off site storage
  (Dropbox, Microsoft Skydrive, Amazon Cloud)

Disaster Recovery Planning

Mayday! Mayday! Mayday!

The computer or data is irreplaceable or business critical.
Recreating the data or rebuilding the computer will take significant time.

- Nightly backups of critical computers
- Nightly or hourly backups of critical data
- Nightly or weekly off site transfers

- Consider real-time backups for the most critical data
  (Acronis, Backup Exec, Livedrive, Dropbox, RAID)

Disaster Recovery Planning

Testing , 1, 2, 3

Test your recovery plan monthly to confirm reliability.

- Verify backup image files

- Review computer backup settings and software for changes

- Check the status of off site storage locations

- Restore a backup image to an alternate location to confirm it works

HOGAN CONSULTING

INTERNET SOLUTION DESIGNERS

Mike Hogan, MBA
256.783.9642
www.HoganConsulting.com