

Cyber-Security

Toby Brown

August, 2003

Outline

Goals

- Scare You Sufficiently
- Show You Some Stuff
- Give You Some Ideas
- Point You Towards a Plan
- Leave You a Little Less Scared

What is Technical Security?

Three Parts:

Physical

Location of servers, locked doors, ...

Human - The biggest threat

The "Disgruntled One"

"Bribing the Guard"

Attention Deficit Disorder

Technology

Firewall , Virus, Intrusion & Auditing

Scaring You

The Inverted Analogy

Mail like E-mail

Office to ISP

ISP to ???

??? to ISP

ISP to destination

Technical Security

Firewalls

Like a moat

Virus Protection

Like a 'Gate Keeper' to files

OS and Application Holes

Like a back-door draw bridge that's been NAILED down

Back-ups

Actually do this first

Firewalls

Software

- ZoneAlarm (free)
- Norton Internet Security (\$50)

Hardware

- Cisco PIX (\$1,500)

Intrusion Detection

- CA Intrusion Detection
- Policy issue too

All in One 'Swiss Army Knife'

- Symantec Security Appliance (\$18,000.00)

Virus Protection

Two Parts

Software

- The Engine

File Library

- List of detectable viruses
- Regular Updates – weekly at least

Note Hoax Viruses

- Teddy Bear – “jdbgmgr.exe”

The “OS” Black Hole

“Not Built With Security in Mind”

- MS – “Security Over Functionality”
- 3 – 5 years

Hack – Alert – Patch

- Patches applied in order!

Application Holes

- The newest threat

Disaster Recovery

At The End, But Really The Beginning

Back Up

- To What – Tape, CD, ...
- To Where – Off-site, Data Center, ...
e.g. AmeriVault

Getting it back – Test it!

A Range

- Weekly to Real Time
- Tape to Spare Site
- Cheap to \$\$\$\$\$\$

Ethics – The Moving Target

Client Confidentiality

- The Third Pillar

- Two Concerns
 - In Transit
 - E-Mail
 - In Storage
 - Your Network
- Standards or Care are Evolving
- Letter of Engagement / Use of Technology

- Protecting the Goods
 - Communication
 - Secure Document Exchange
 - e.g. CaseData SSL Relay
 - Secure e-mail
 - e.g. Zendit
 - Storage
 - Policies and Procedures!
 - Third Party Solutions
 - e.g. NetDocuments

- Growing Concerns
 - Wireless LANs
 - Speed vs. Security
 - “War Driving”
 - Hackers
 - Are You a Target?
 - “Script Kiddies”
 - Portables – PDAs, Phones, ...
 - Secured?
 - ASU Case

- Paper vs. Electronic
 - Metadata Problems
 - Hidden in MS Documents
 - “Properties”
 - Reviewing, Versioning, Comments
 - Should you look?
 - Deleted documents
 - Still there
 - Backed up too
 - Discarded Computers
 - Game for MIT Students

- Some Discovery Issues
 - Requests
 - Preservation of Evidence
 - What to Request and Costs

Spoliation

Opposite of Security

Handle with Care

Native Files Produced?

Metadata again

The Policy Wrap Up

Internal

Procedures

How you manage tech resources (V = Maine)

Destruction of E-Info

Staff Issues:

Employee handbook policies

Termination procedures

Email & Internet usage

Network privileges

Data access

... and More Policies

External

Privacy

How you interact with clients

Security

How you protect client's data

Upcoming Policy Speed Bumps

Archiving & Destruction

GLBA, HIPAA, S-O, Patriot Act

E-Signatures

Conclusions

There Is Cause For (Some) Concern

Lawyers Need to Protect Information

Ethical Duties

Education is Good

Cost Effective Tools Are Out There