Business continuity

Protecting your systems in today's world

Introduction

- Lee Drake, OS-Cubed, Inc.
- Contact: ldrake@os-cubed.com
- Phone: 585-756-2444
- 30 years of support

LOL Cat warning

Warning – this presentation contains the occasional LOLCAT courtesy of www.icanhazcheeseburger.com

Fair warning of bias… ☺

OS-Cubed is currently a:

- Symantec Partner
- HP Partner
- Microsoft Gold Certified Partner
- Cisco/Linksys Registered Partner

  While this presentation will consider protection strategies in general these are the products we have the most familiarity with. They are certainly NOT the only solution

Today's Security Environment

- Greater interconnectivity exposes more security risk
- New types of security risks
- Business dependence on IT systems means downtime is more expensive
- Limited availability and high cost of experienced IT means all repairs cost more

“Small Business” definitions

- For this presentation “Small Business” will be categorized into the following sizes:
  - 1-5 “home-based business”
  - 5-20 “Small Business”
  - 20-100 “Medium business”
  - > 100 large business (from an IT point of view)

What are the threat vectors

- Direct Internet connection
- Email
- Your website (separate connection)
- Your employees
- Yourself
- Hardware or software failure or corruption

Downtime – you can’t afford it

Is it really a threat?

Computer security costs $$ - directly to your bottom line

- TJ Maxx = $100/released record = $4,500,000,000
- Average of $600 to recover a computer after infection
- Cost to prevent $100-200/year
- By 2011 4% of revenue could be spent on security (10x today's spend

Malware

Threats defined

- Malware – virus, rootkit, spyware
  - Install invisibly
  - You may be infected
  - Botnet infection slows down your computer and takes up internet bandwidth – sending spam or infecting other computers
- Recent documented infection shows 200,000 bank accounts and CC# exposed!

Business Continuity

- Protect your data and your productivity
- Downtime costs money, and can lose you opportunity
- Data loss is more costly than the downtime
- Two types – full disaster recovery, and systems recovery

Information leakage

- Losing information to competitors
- Losing information to employees who leave
- Privacy issues
  - Medical (if in that industry)
  - Credit card/Customer privacy
  - Employee privacy (HR)

Information Sabotage

- Employee sabotage
- Competitor sabotage
- Unintentional damage

Productivity loss

- Employee “surfing” during work hours
- Improper use of bandwidth (Music sharing sites, etc.)
- Gaming, “solitaire” etc.
- Slowdowns due to malware/spyware
- Spam processing

The good news

- With a proper set of tools, protecting yourself does not have to be difficult or time consuming
- Recent advances have lowered the cost of protection significantly
- New technologies make it easier to deploy and manage

Tools

Perimeter control Tools

- Required
  - Spam blocking systems
  - Firewall
- Optional
  - Content management
  - VPN/Encryption
  - Network access control
  - All-in-one devices

Endpoint Protection

Tools

- Endpoint protection (all required)
  - Virus control (formerly antivirus)
  - Spyware
  - Personal firewall
  - Personal spam control
  - Endpoint protection (all of above)

Tools

- Business continuity
  - Tape backup
  - Online backup
  - Disk to disk backup
  - Network Attached Storage
  - Offsite storage
  - PC Backup

  - (one onsite, one offsite required)

HR Practices

Tools

- System management and monitoring tools
- HR Best practices
  - Employee manual (Required)
  - Manager training
  - Employee orientation sessions
  - Employee termination procedures

Backup and fail in that order!

Backup explained

- With low price USB, Firewire and Network Attached storage devices the landscape for backup has changed
- Backup to disk is fast, reliable and allows almost instant restore and rebuild – even over a network
- New disk imaging products allow “snapshot backups” for instant restore

Symantec Ghost/Backup Exec System Recovery

- Every important computer in your organization should be protected by Ghost or BESR (corporate version)
- Reduces recovery time for even a total disaster to a couple hours
- Backups are faster, more reliable and easier, require no human intervention
- Can be used for offsite

Still need offsite backup

- Protects asset in the case of total destruction of server room (natural disaster, fire, sabotage, etc)
- Can be used as history for deep-restore
- Snapshots of business at various points.

Offsite backup options

- Online options
  - Require significant bandwidth – do not underestimate requirements
  - Restore times frequently longer and can be more complex
  - Frequently do not backup system state – files only
  - Require a monthly fee for storage, that increases with the amount stored
  - If you trust 3rd party vendor can be more secure

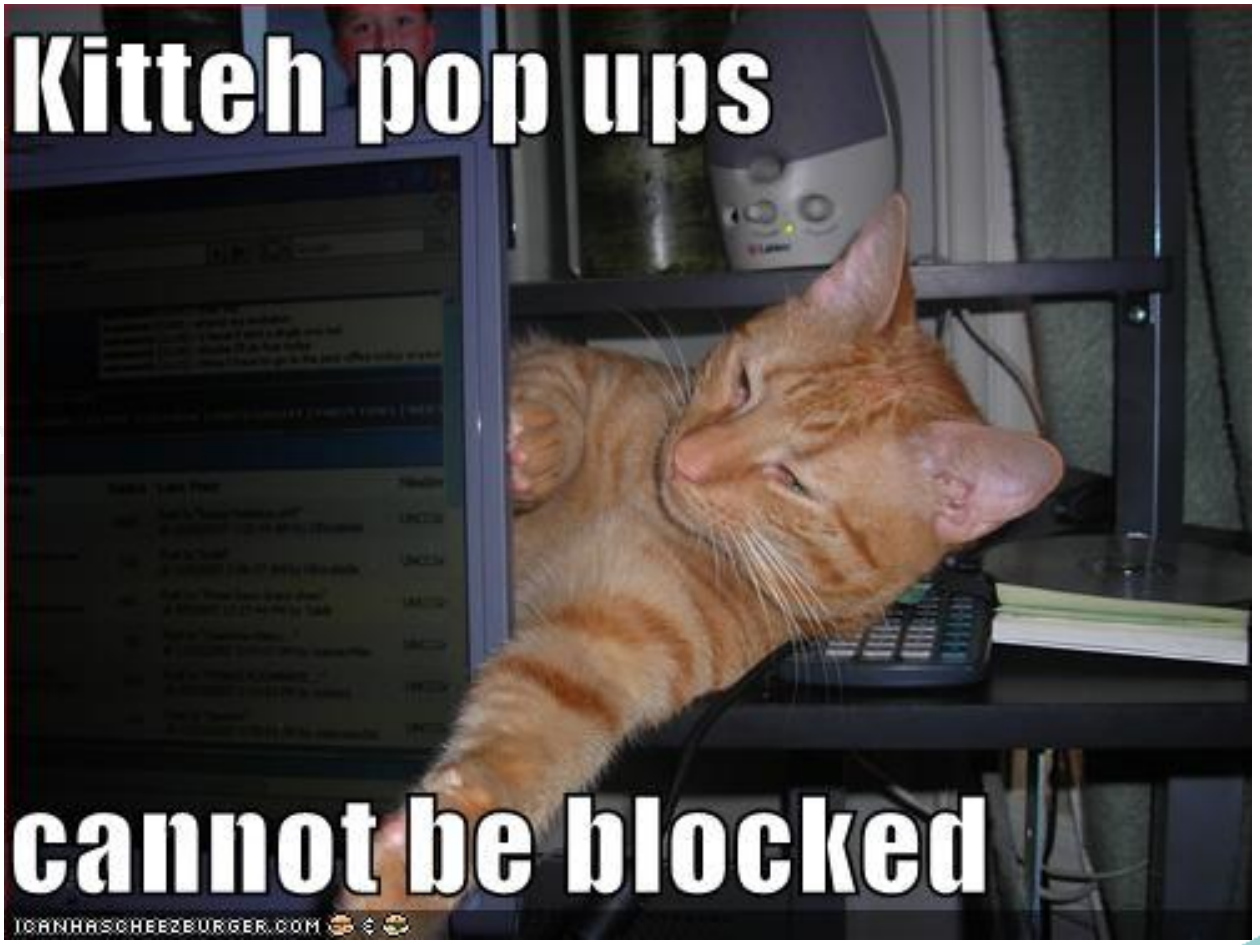
Offsite Backup options

- Tape
  - Compact size makes off-site easier
  - Backups require physical intervention (changing tapes)
  - Tapes deteriorate and need to be changed out every 1-2 years for new tapes
  - Can represent a security risk if stolen
  - For a monthly fee Iron mountain will retain, store and exchange tapes

Offsite backup options

- Taking USB drives offsite
  - More attractive as drives size shrink to that of tapes
  - Drives much more susceptible to environmental damage
  - Similar downside characteristics as tape
  - Requires “human intervention”
  - Can be a solution for home businesses

Endpoint Protection



Endpoint protection defined

- Controlling what happens at the workstation
  - Virus protection
  - Spyware protection
  - Device control (usb drives, other attachable devices)
  - Workstation firewall (software firewall)
  - Initial access to the network
  - Can include email client based spam control

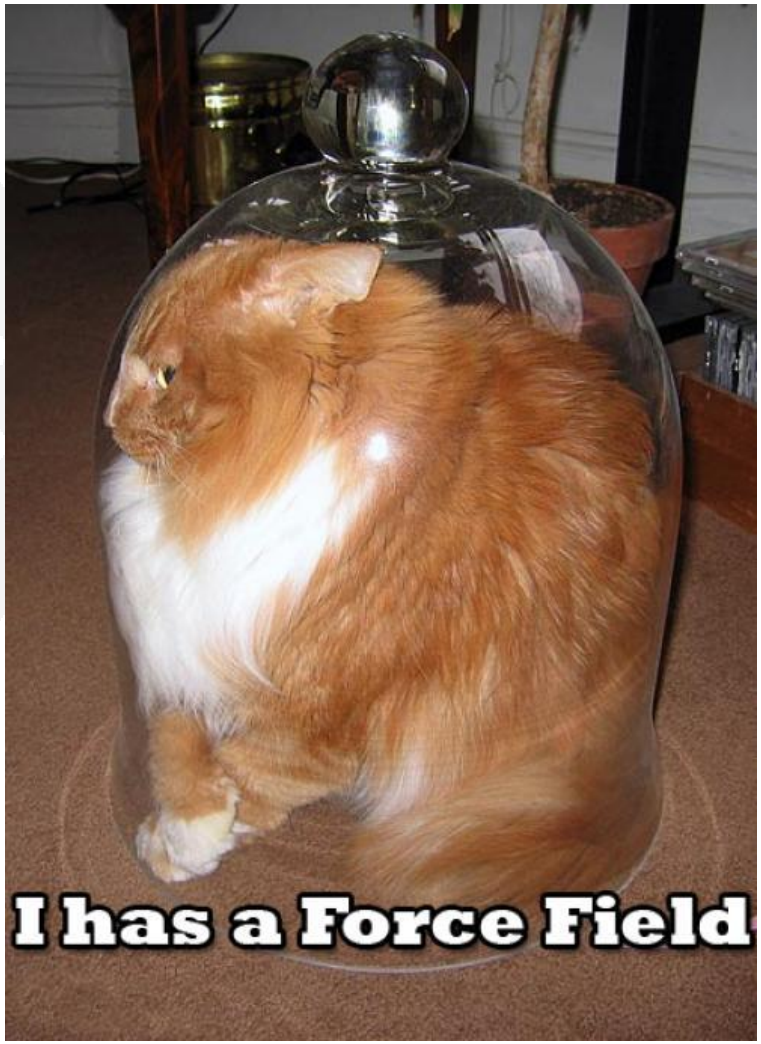
Endpoint protection options

- 4-5 major players in this space
- Features and capabilities frequently leapfrog
- Best advice is to pick one and stick to it, don’t swap back and forth
- Major providers include: Symantec, McAfee, AVG, CA, and Kapersky
- Symantec 2008 got PC World top spot

Don’t overdo it…

- Multiple products to protect your endpoint are generally NOT needed
- Use one product for best results, easiest management and fastest speed
- Multiple products slow your system down by doing repeated tests
- Use of clean-up products should be limited to infected machines

Protecting your network



Firewall appliances

- Firewalls and content management systems prevent direct hacking from outside world
- Can be used to control what resources your internal users can reach in the outside world (CM)
- Are your first line of defense against hackers

Perimeter Firewall limitations

- Once something is behind the firewall, it can spread quickly
- Wireless access points behind firewalls are susceptible to hacking attempts
- Trojans and other malware operate from behind the firewall and can be difficult or impossible to block as their traffic looks like web traffic

Endpoint firewalls

- Firewalls at the client can prevent spread behind the corporate firewall
- Endpoint protection typically includes a firewall at each client
- Windows comes with a built-in firewall at each client, which should be on (at a minimum)

Spam Control

Other appliances

- Spam control appliances sit between you and your email server, or between your email server and the world
- They allow constantly updated spam signature and source control
- Can significantly reduce spam-load
- Can be expensive to configure and maintain – higher risk of false negatives.

Other appliances

- VPN – Virtual Private Network
  - Extends your network to home or mobile machines
  - VPN connected machines should be subject to the same rigorous security requirements as internal machines
  - Can allow work from home easily
  - Frequently built into perimeter firewalls
  - Are even affordable at home office prices, but require a fixed IP address (not a home account)

Other stopgap methods

- Use an alternate browser (Firefox, Chrome etc.) – however ALL browsers have security issues
- Use an alternate OS – Linux and Mac OSes have a limited audience, thus are not targets. ALL operating systems have vulnerabilities though
- Properly configured and patched any of these can be secure

Updates and patches

- You or your provider should frequently check for and apply new patches
- Subscribe to Microsoft and/or Symantec RSS feeds for emergency security bulletins
- Select ALL critical updates, and any security or stability related optional updates
- Run updates manually every other month

Network Administration

HR Guidelines

- Every company should have an employee manual that details:
  - What is considered appropriate internet use
  - Specific consequences of inappropriate use
  - Rules about using copyrighted and unlicensed materials, pornography, etc.
  - Email use policy
  - Note that there is no expectation of privacy
  - A policy regarding use of unapproved software
  - A reminder that data tampering is a federal crime
  - A nondisclosure agreement regarding company data

Drive security

Physical security

- USB drives change everything
  - Exposure risks from downloading data goes up
  - Can “boot to USB” and gain access to files without the OS or Endpoint loaded
  - Can put browser and files on usb drive and surf anything anywhere without installing on PC
  - Should seriously consider locking USB to read-only status

Do you trust your vendors?

- All your vendors – not just IT vendors
- I've seen server rooms where contractors are working unattended
- Do not assume because of someone's job that they're not a computer hacker

Server rooms should be locked

- Access to key trouble points should be locked from employee access
  - Network hubs and switches
  - Servers and network appliances
  - Routers and firewalls
  - Detachable USB drives and tapes

Password security

Password security

- Passwords should be at least 8 characters
- A combination of letters and numbers
- Something people can remember
- Don’t make them change them too often or they’ll just write them down

Fingerprint authentication

Fingerprint authentication

- Finally a valid solution with newer, cheaper technology
- Works best with Window's Vista's ability to have multiple users logged on simultaneously

What about encryption?

- For sensitive data it can be invaluable
- MUST have a safe and accessible place to look up the password in case it is lost or you are hurt
- Data will be UNRETRIEVABLE without the password
- Can affect the validity and availability of backup data

Do you trust your protection?

Home Business typical configuration

- Under 5 users
  - Inexpensive firewall (no content control – sonicwall/linksys/netgear)
  - Retail endpoint protection (Symantec, AVG, Etc.)
  - Endpoint spam control, or use 3rd party service
  - Ghost for individual workstations
  - NAS for in-house backup
  - USB Hard disk exchanged offsite for offsite backup

Small Business typical configuration

- 5-20 users
  - Centralized computer server
    - Tape backup for offsite
    - Centralized licensed endpoint protection
    - Depending on email – either centralized virus and spam or endpoint
    - NAS for localized emergency recovery
  - Endpoint protection at systems
  - Mid-range firewall/spam/content (Sonicwall, Cisco) plus OpenDNS

Medium Business typical configuration

- Perimeter
  - Firewall – both directions (Cisco, Sonicwall)
  - Content management appliance or OpenDNS
  - Spam control appliance (Barracuda)
- Server
  - Centralized endpoint protection
  - Centralized systems management and monitoring
  - Protected by local disk imaging and tape or offsite backup
- Endpoint
  - Endpoint protection
  - Local disk imaging of key systems

Large business

- Best advice is to hire a security expert to design a system for you
- Recommend going with specialized appliances
- Limiting the number of different vendors simplifies management
- Solve with an overall approach not individual band-aids

Notes can be found…

- On my website www.os-cubed.com
- Off my linked in and facebook accounts (Search for Lee Drake in both)

Contact Information

OS-Cubed, Inc.
Lee Drake, CEO
274 Goodman St. N, Suite A401
Rochester, NY 14607
Ldrake@os-cubed.com
www.os-cubed.com