



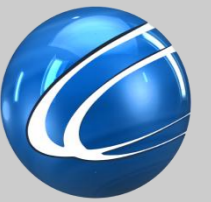
columbus  
business solutions



# Protecting Digital Assets in the Knowledge Economy

Horace Sookdeo, CISSP  
Pre-Sales Manager  
Columbus Business Solutions

# How Secure Are Your Information Assets?

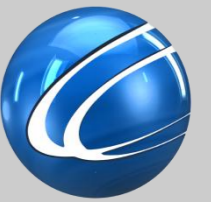


- Have you updated the latest patches and revisions?
- How do you make sure your policies and procedures are being followed?
- Do you proactively monitor your network?
- Have you hardened your servers?
- Is there an intrusion detection system in place?
- Do you know where your vulnerabilities are?
- How often do you try to hack your own network?

## Columbus Security Solutions

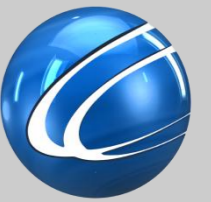
Managed Firewall, Virtual Private Network (VPN),  
Data Loss Prevention (DLP), Ethical Hacking

# Why You Need More Than Perimeter Security



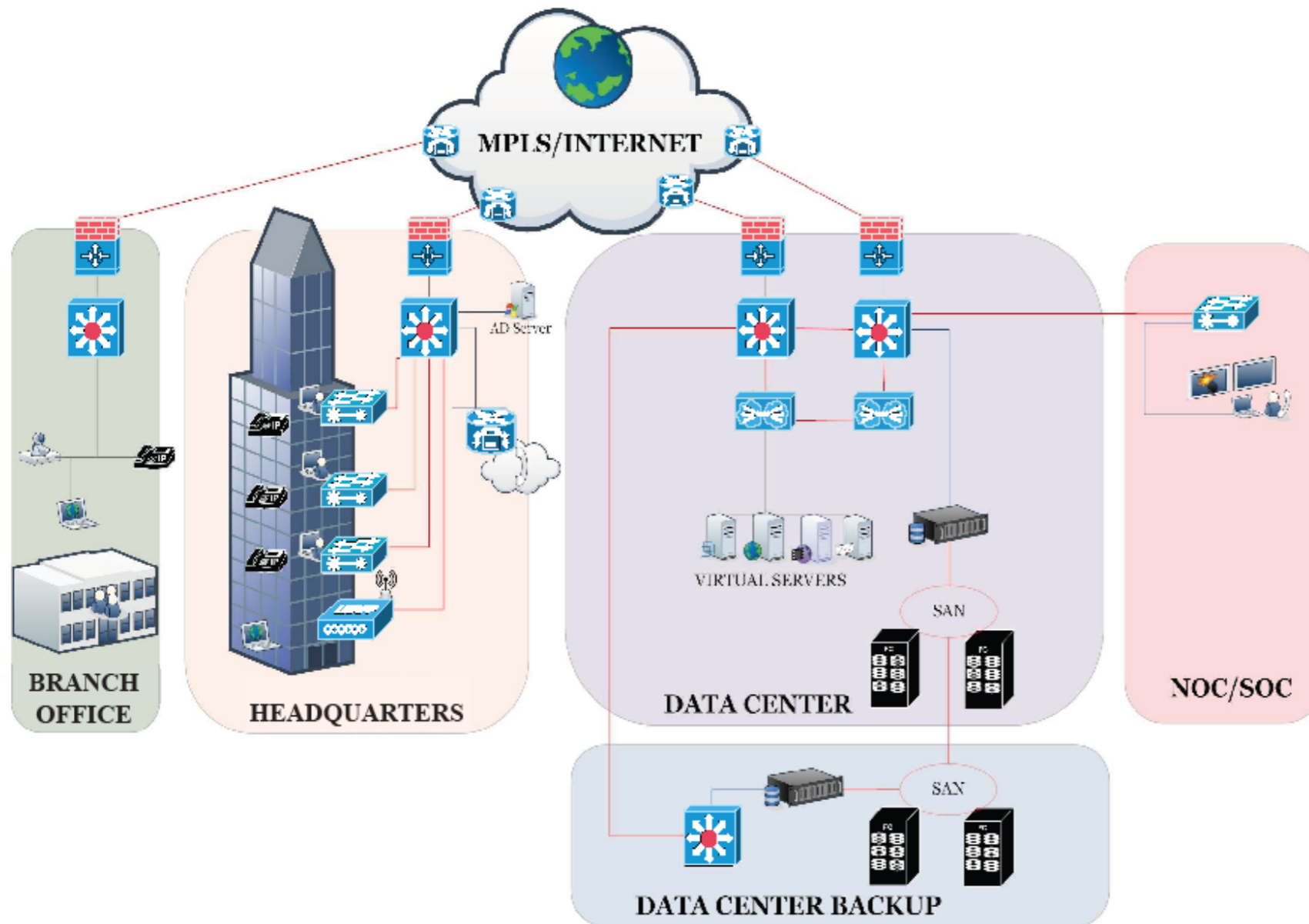
- Companies invest significant resources in firewalls, intrusion detection/prevention systems, sophisticated anti-virus, spyware and content filters solutions.
- These protect the perimeter, but what about usernames, passwords, and confidential information?
- More and more often consumers find themselves victims of email scams, phishing, and malware infections coming from infected sites.
- The Anti-Virus, Anti-Phishing, Anti-Spyware, personal firewall and intrusion prevention systems are crucial to your laptops? Do you have them? Are they up to date?
- Consumers are not regulated

# Security Goes Beyond the Perimeter



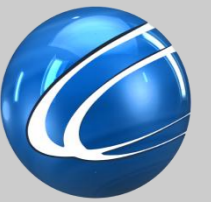
- The perimeter has extended to each users computer
- End users can be victims of identity theft and/or fraud if their computers are compromised
- Conduct threat analysis and vulnerability assessments
- Identify risks and make decisions based on clients' unique characteristics
- Focus on protecting key information assets by identifying security requirements
- Help develop Security Policy and make recommendations on security mechanisms
- Help implement security recommendations
- Develop practice-based risk reduction strategies using internal and external sources with 24x7x365 security monitoring

# Columbus High-End Security



Perimeter	IDS / IPS SVPN
Servers	Monitoring
End Users	Data Loss Prevention (DLP)

# Data Center requirements



Data Security



Diverse Path and Physical Link Redundancy



High Availability



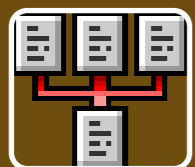
Dedicated WAN links



Off island datacenter outside hurricane zone

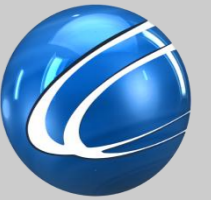


Class of service enabled network (MPLS)

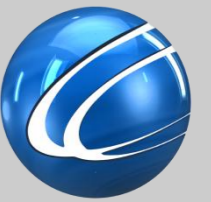


Ability to add /enhance services (i.e. VoIP, Wireless, Firewalls, Video Conferencing)

# Secure Managed Solutions

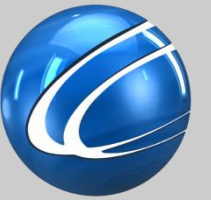


- High-performance managed security solution
- Virtual Private Networks and Firewalls
- Columbus's 24x7 proactive monitoring
- Hardware and software set-up and on-going maintenance.  
Timely OS revisions and patches
- Incident response services
- Aggressive Service Level Agreements (SLA)
- Spans the entire enterprise – from headquarters to branch offices to remote and mobile employees – enabling highly secure enterprise-wide networks.
- Expert security policy configuration and management
- Security reports and advisories



# Secure Virtual Private Networks

- Communicate with branch offices or business partners over a private IP backbone or the Internet
- Robust remote access through IPSec-encrypted tunnels and digital-certificate, RADIUS, or secure-ID-based user authentication
- Cost effective, enterprise-class secure communication solution for organizations with multiple remote offices and locations
- Send and receive information securely without installation, maintenance, monitoring, or management worries
- Market leading software from Cisco, Check Point, Nokia, IP Security, Netscreen, and many others
- Increase the security and accessibility of your corporate applications from both remote users and branch offices
- Easily and more securely extend your network to partners, suppliers, and customers



- To catch a hacker...Think like one. Highly skilled security professionals will follow the same methodology that an outside attacker would use: gather information about the systems, do low-level scans, catalog possible vulnerabilities, and attempts to exploit, elevate privileges and leverage initial successes to expand influence
- Assurance and peace of mind that periodic scans get done
- Current information on new security issues applicable to clients' networks
- Ongoing maintenance services with timely operating systems revisions and patches
- Monthly security reports and advisories

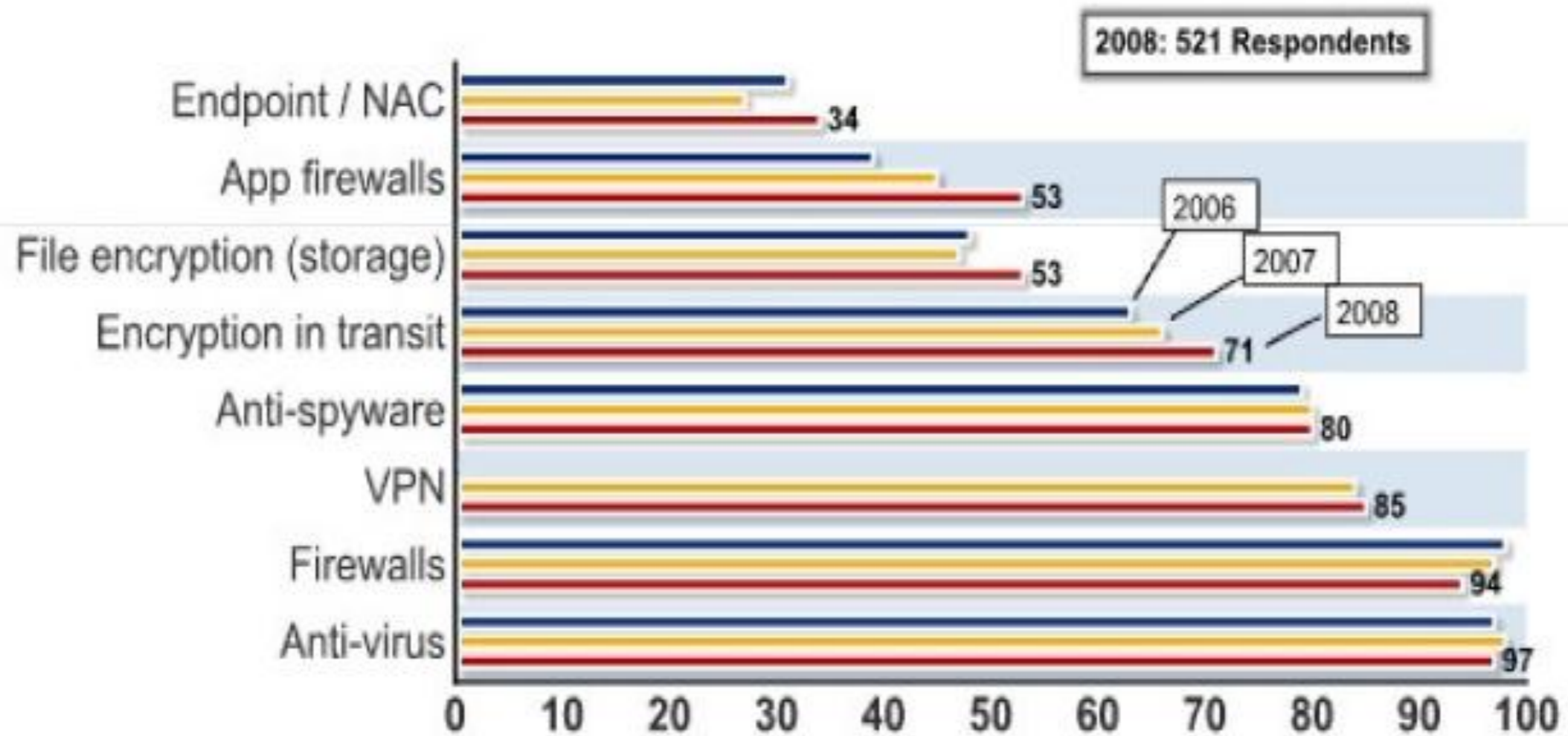
# How Secure Is The Provider's End?



- Most providers connected to the Internet are required to have firewalls and intrusion detection/prevention systems
- These systems can not only control the access but also identify attacks as they are occurring.
- Companies often spend significant resources implementing sophisticated anti-virus, spyware and content filters solutions to protect their perimeters.



Figure 16: Security Technologies Used



Source: Computer Security Institute

# Isn't This Enough?



- One may think that the perimeter is strongly protected.
- We build a concrete house, added fences and even alarm systems. One question remains: who has the key?
- If the provider protects its network perimeter: are YOU protected?
- Is your username, password, and confidential information at all protected?

# What Really Happens Underneath?



- Although the communication between a client and a server is protected the content of their session is not.
- Web applications are extremely sensitive to input validation errors making them easy targets to upload malware.
- Once web sites become infected they make themselves available for infecting all customers that connect to them.
- This, combined with Social Engineering techniques such as Phishing and Spam Email sets the tone for wide spread malware infections.



# How Secure Is the Consumer End?

- More and more often consumers find themselves victims of email scams, phishing, and malware infections coming from infected sites.
- The Anti-Virus, Anti-Phishing, Anti-Spyware, personal firewall and intrusion prevention systems are crucial to your laptops? Do you have them?
- Consumers are not regulated and insurance companies don't encourage them to buy security.
- So where is the security problem?



# Conclusions

# Security Goes Beyond the Provider's Perimeter



- Protecting the provider's perimeter is not enough in this new security paradigm.
- The perimeter has extended to each users computer.
- End customer can be victims of identity theft and/or fraud if their computers are compromised.
- The end customer expects retribution from the provider.
- The provider **MUST** work closely with the customer to defeat this new security risk trend.



# What Can the Provider Do?

- Conduct threat analysis and vulnerability assessment.
- Identify risks and make decisions based on their unique characteristics
- Focus on protecting key information assets by identifying security requirements
- Develop Security Policy and make recommendations on security mechanisms.
- Implement security recommendations.
- Develop practice-based risk reduction strategies using internal and external sources with 24x7x365 security monitoring.



# What Can the End User Do?

- Protect your computer and your assets.
  - Add all necessary security software to protect against all known attacks
  - Avoid unknown emails and don't trust all web sites in the Internet.
  - Keep your security software up to date.
- Report any suspicious activity to your provider immediately.
- Contact law enforcement agencies as needed.



columbus  
business solutions



Thank you.