

Experience Today the
Network of Tomorrow.

Cisco Expo
2009

Threat Defense



Tariq Ahmed
Security Manager
Emerging Markets

Welcome to the Human Network.

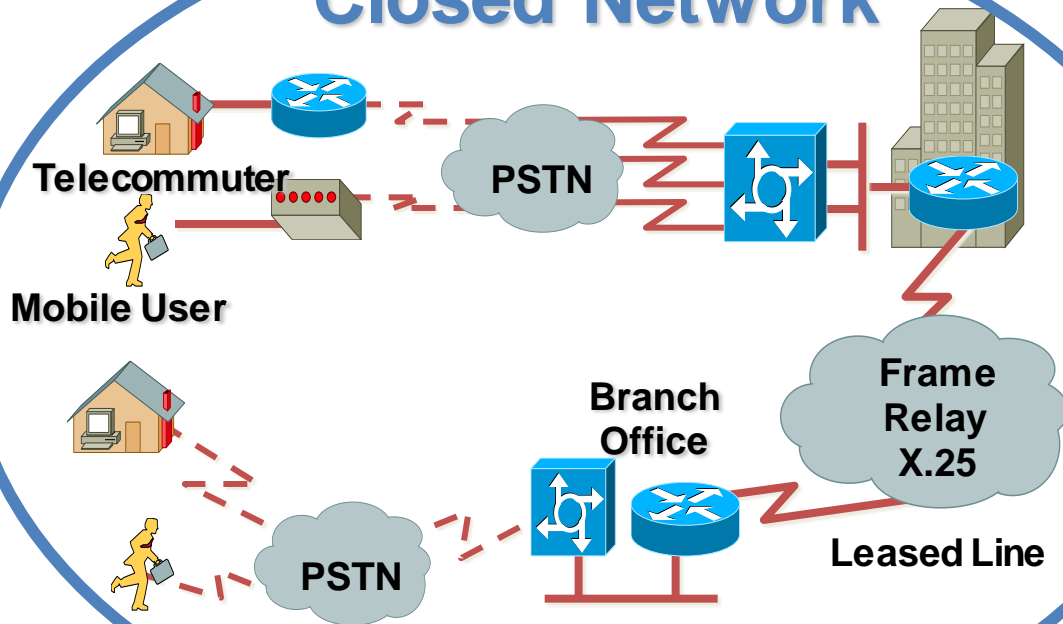


The Changing Landscape



Networks Of The 90s

Closed Network

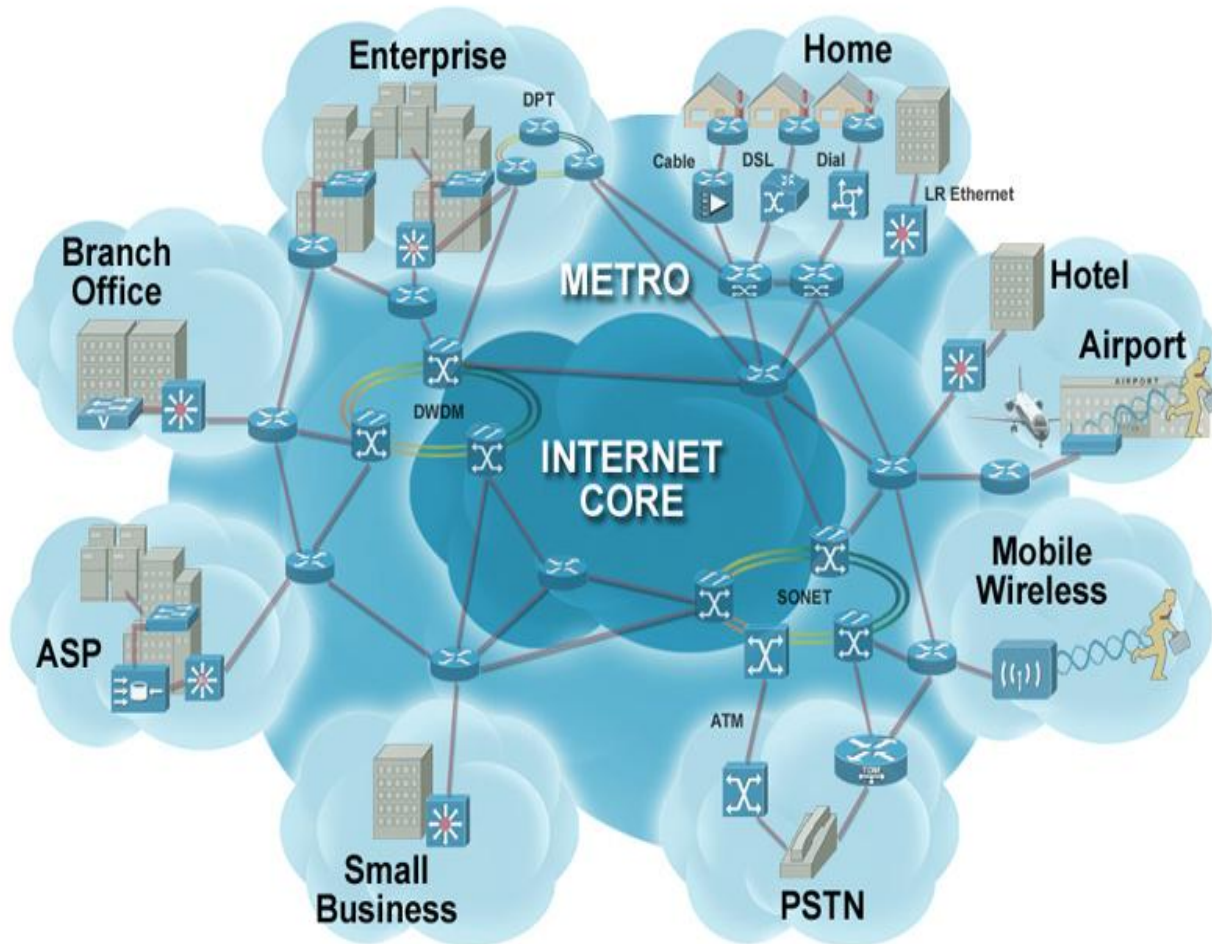


Characteristics

- Isolated and trusted environments
- Secure the few public WAN connections
- Secure hosts with Anti-Virus

Most security devices were designed to secure networks like this

Networks of the 00s



Characteristics

- Distributed Internet connections to secure
- Need to open up data centers for more ubiquitous access
- Dramatic increase in employee mobility
- Increased use of new campus technologies like WLAN & IPT that provide more network access methods
- Growing damage due to viruses & worms

But networks of 2000 are changing and security demands are different

The Changing Data Landscape

Today's Work Environment
Is Changing

Collaboration is a Business
Advantage

Increasing Regulatory and
Governance Pressures

More Data Is Lost or Stolen*

*Attrition.org Data Loss Archive and Database



Personal Use of Company-Issued Computer

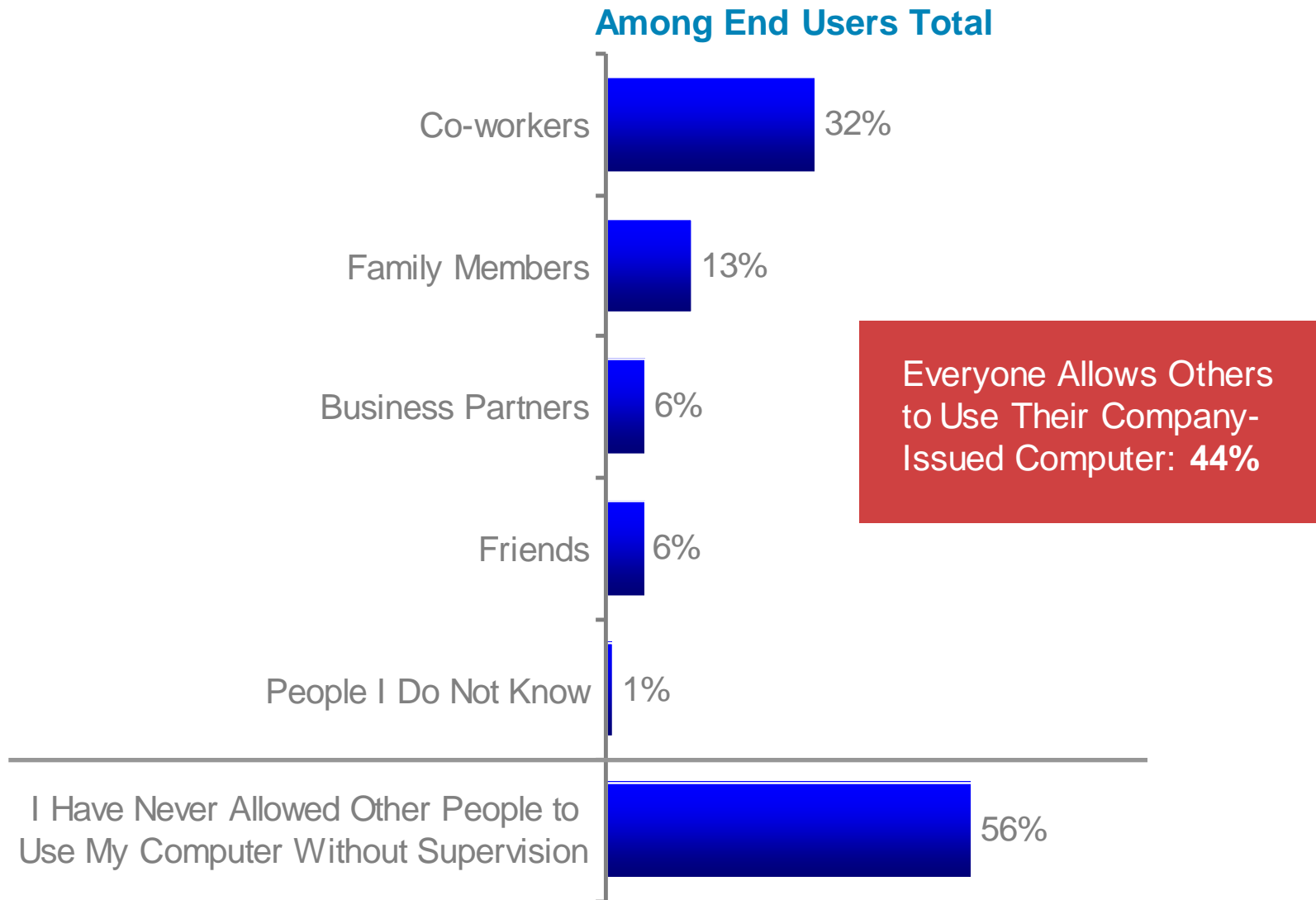
Q: You indicated that you use your company-issued desktop or notebook computer for personal matters. Please indicate what types of personal activities you conduct on a regular basis: for example, at least once per month.



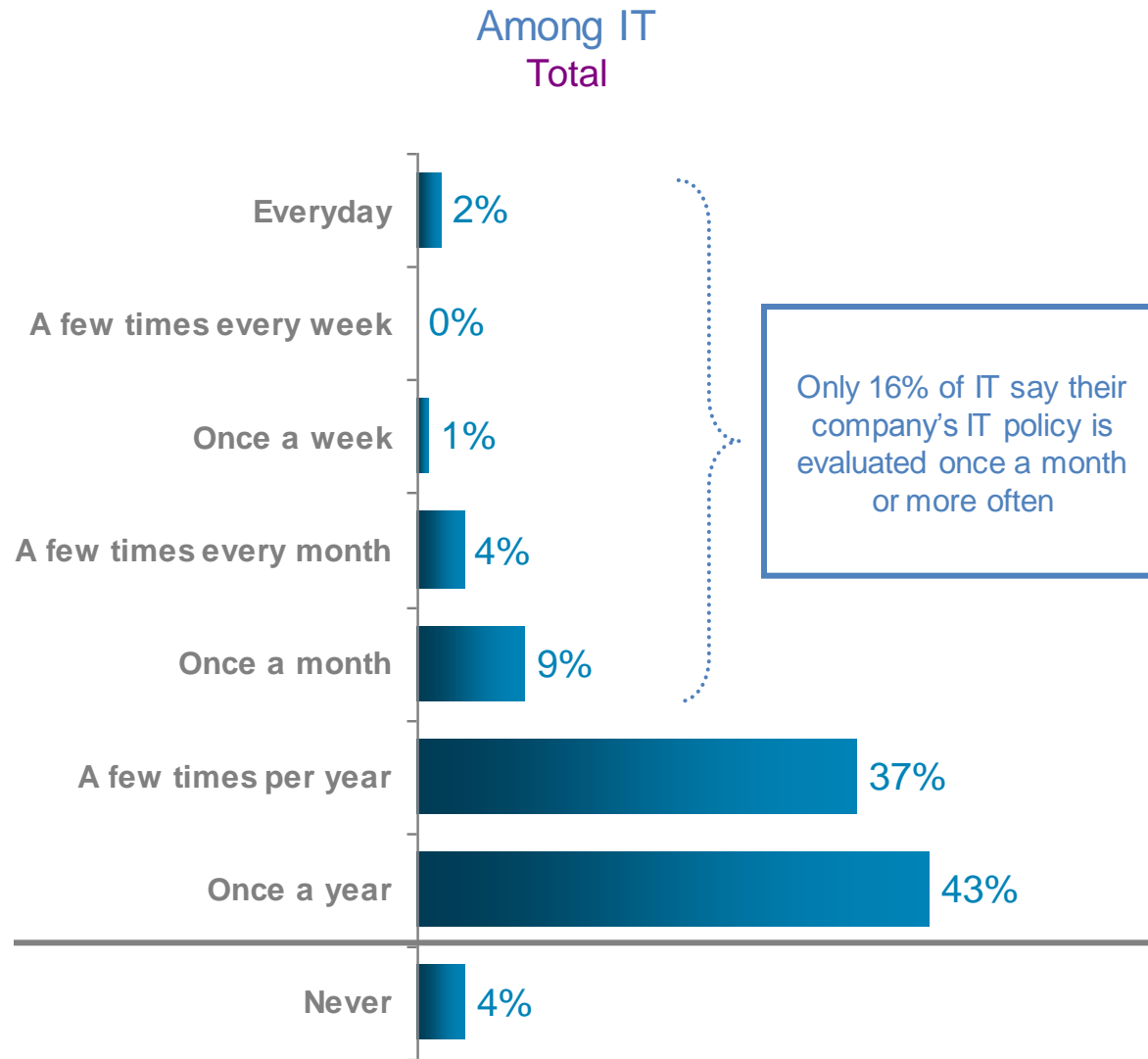
Personal Use of Company-Issued Computer

Personal Email Using Personal Email Account	78%	Online Bill Paying	36%	Social Networking : MySpace, Facebook, Etc.	15%	Chat Rooms	9%
Web Surfing	52%	Internet Shopping	36%	Blogging	13%	Online Gambling	3%
Online Banking	48%	Instant Messaging	35%	Online Investing	11%	Non appropriate	1%
Personal Email Using Work Email Account	42%	Music and Video Downloads	17%	Person-to-Person File and Picture Sharing	10%	Other	3%

Do you share Sharing Company-Issued Computer with Others?



Frequency of Corporate Security Policy Evaluation



Security Now a Baseline Architecture for All Communication Technologies



Factors That Impact Business Security



Collaboration and Communication

- TelePresence / Video / IM / Email
- Mobility
- Web 2.0 / Web Services / SOA



The New Threat Environment

- The Eroding Perimeter
- Spam / Malware / Profit-Driven Hacking
- Data Loss and Theft



The Business Impact of Security

- IT Risk Management
- Regulatory Compliance
- Security as Business Enabler

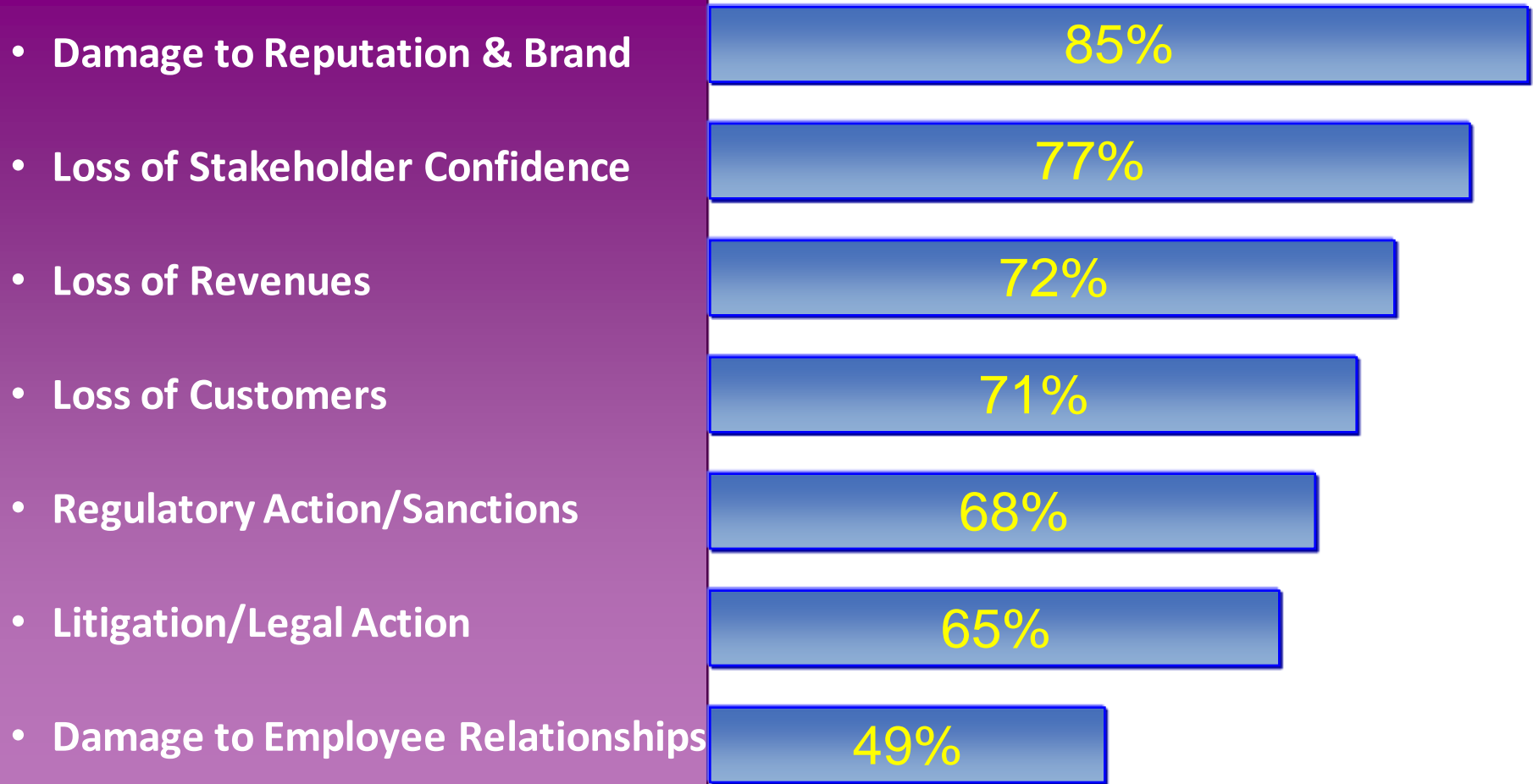
Top Concerns in 2009

Limited Budget	61%
Compliance with government security and privacy regulations	57%
Educating executives on risks/issues	53%
The scope/volume/proliferation of data that needs to be protected/devices that need security	51%
Not enough security staff	47%
Wireless LANs	30%
Mobile clients	28%
Company growth	28%
Volume/complexity of network traffic	27%
Lack of key security skills	25%
Security outsourcing	9%
Other	8%

Q12. What are the top three security challenges facing your company during the next 18 months? (base: 477)

- **Application vulnerabilities** allow hackers to gain access to underlying databases and improper levels of access to applications
- **Improper data access** through improperly configured firewalls and legacy firewall technology
- **Operating system vulnerabilities** allow hackers control of computers and enable information theft and improper system access
- **E-Mail** can offer spoofed links (e.g. phishing) and attachments infected with spyware, viruses, and other malware
- **Internet use** introduces files through download, drive-by installations, and errant software installations
- **User access** to information and resources that they either shouldn't have or don't need
- **Network system vulnerabilities** can allow hackers to take over entire domains (pharming)
- **Human error** due to mistakes, not following corporate policies, using detachable hardware etc.

Leading Business Consequences of Information Security Incidents



** Source: Ernst & Young's 2008 Global Information Security Survey*

What Is Data Loss Prevention (DLP)?

- DLP: Security measures to protect confidential and private data
 - - in-use
 - - in-motion
 - - at-rest
- From both intentional and accidental loss of data



Cisco DLP Solutions – Four focus areas

- Data-In-Motion
 - Email
 - Network access
 - Wireless
- Data-at-Rest
 - Portable/Removable media (USB)
 - Authorized abuse
- Data-In-Use
 - IM
 - File share
 - Web uploads
- Compliance Regulations
 - Customer credit card information
 - Medical Information
 - Financial Information



Data Loss Prevention

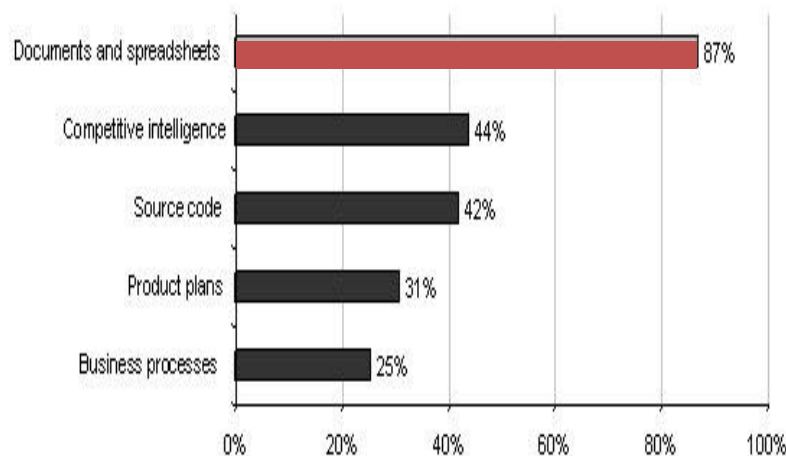
Business drivers : Intellectual Property Protection



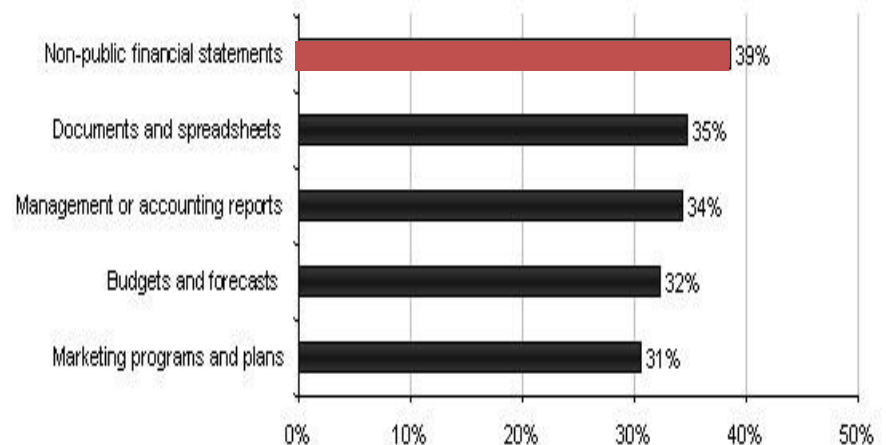
Every company needs to protect some intellectual property

- ✓ Trade secrets, Source code, merger & acquisition plans,
- ✓ Financials (forecasts, budgets), Competitive intelligence
- ✓ Processes & plans

What intellectual property creates the greatest risk to your organization if lost or stolen? ³



What business confidential information creates the greatest risk to your organization if lost or stolen?



Solutions



Making the Journey from Point Solutions to Self-Defending Networks

- Self-Defending Network: best of breed products, systems-based approach
- Helps provide solutions for business security
- Risk gaps are reduced; complexity is reduced; total cost of ownership is lower
- Protect, optimize, and grow your business



Requirements: Visibility and Control



Firewall and VPN

- Traffic access control
- Encryption



Intrusion Prevention

- Detection
- Precision response



Content Security

- Email Spam
- Web filtering

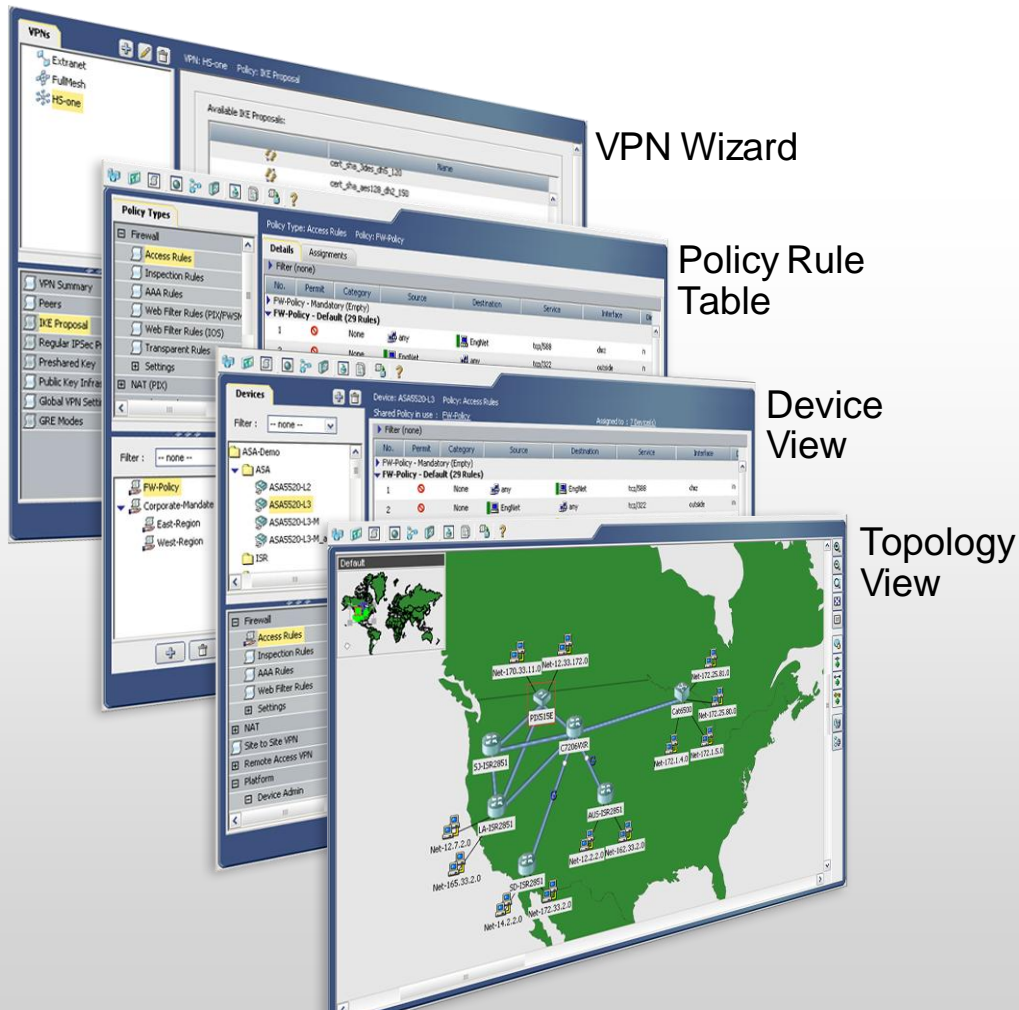


Endpoint Security

- Host IPS
- AV solutions

Centralized Policy Management and Monitoring

Cisco Security Manager



- Unified services management for security including firewall, VPN, and IPS
- Intuitive, feature-rich user interface
- Different views for different administrative preferences
 - Device View
 - Topology View
 - Policy View
- Efficient management architecture for large-scale security deployments

Centralized Policy Management and Monitoring

Cisco Data Loss Prevention

An Integrated Approach to Data Loss Prevention through Security

- **To protect against confidential data theft and loss, a multi-layered security foundation is needed**
 - ✓ Control/limit access to the data – firewalls, remote access controls, network access controls, physical security controls
 - ✓ Secure information from threats – protect perimeter and endpoints from malware, botnets, viruses, DDoS, etc. with security technology
 - ✓ Control use of sensitive data once access is granted – policy-based content inspection, acceptable use, encryption
- **Cisco's Solution for Data Loss Prevention**
 - ✓ Build a secure foundation with a Self-Defending Network
 - ✓ Integrate DLP controls into security devices to protect data and increase visibility while decreasing the complexity and total cost of ownership of DLP deployments

Cisco's Self-Defending Network

DLP Core Products

New

System Management

Policy—Reputation—Identity

Application Security

Content Security

Network Security

Endpoint Security

Cisco Security Manager
Cisco Network Compliance Mgr

ACE Web Application Firewall

IronPort Web and Email Security

Cisco Network Access Control

Cisco Security Agent 6.0

Cisco Storage Media Encryption

Cisco Self-Defending Network:

Best of Breed Security in a
Systems Approach

Cisco DLP User Cases



Cisco Expo
2009

Welcome to the Human Network.



DLP Data-in-Motion

Company confidential data accidentally

Accidental data loss over email can occur simply by using Outlook's AutoComplete

Scenario

- One of Eli Lilly & Co.'s outside lawyers at Philadelphia-based Pepper Hamilton had mistakenly e-mailed confidential Eli Lilly discussions to Times reporter *Alex Berenson* instead of *Bradford Berenson*, her co-counsel at Sidley Austin, costing Eli Lilly nearly \$1 billion.
 - January 2008 <http://www.portfolio.com>



Cisco Solution

- With IronPort C-Series
 - Enforce email communication between authorized parties with policy-based encryption, including user authentication and key delivery.
 - Recall email if it is inappropriately delivered to the wrong business partner with the Email Recall feature.
 - Monitor and block emails containing sensitive keywords, so that a document filled with critical data types sent to a non-business partner triggers a DLP violation

DLP Data-in-Motion

Private data accidentally sent out via email

Prevent sensitive data from being sent to unauthorized parties, which can occur by selecting the wrong attachments or sending to the wrong email distribution list or recipients.

Scenario

- The Ohio State University Agricultural Technical Institute accidentally sent an e-mail containing personal faculty and staff information to about 680 students. The e-mail had an excel attachment that contained names, positions, salaries and Social Security numbers on 192 faculty and staff members. In a follow-up e-mail students were asked to delete the e-mail that contained the personal information.



Cisco Solution

- With IronPort
 - Filter all mass or bulk outbound e-mails and attachments for sensitive data such as Social Security Numbers, Credit Card Numbers or any administrator-specified text.
 - Enforce policies to encrypt, deny, or report based on the restricted data found in e-mail attachments.
- With Cisco Security Agent
 - Monitor sensitive files on desktop and prevent files from being uploaded in email client.

DLP Data-in-Motion

Data Loss through a Wireless Breach

Protect against data theft and confidential and private data loss through unauthorized users accessing internal networks through an insecure wireless infrastructure.

Scenario

- More than 45M customer credit cards numbers were stolen from retailer TJX and used to buy over \$8M worth of merchandise. Thieves were able to access data streaming between handheld price-checking devices, cash registers and the store's computers through a wireless breach. TJX had an outdated wireless security encryption system and had failed to install firewalls and data encryption on computers using the wireless network.



Cisco Solution

- Cisco's Wireless LAN Controller delivers secure wireless connectivity to protect from breaches.
- Cisco's Wireless Control System detects rogue access points to protect against unauthorized computers from accessing the network.
- Cisco NAC enforces that the systems connected to the network are using the latest wireless security policy.

DLP Data-in-Motion

Data loss through Web browsing

Prevent data loss from web browsing.

Scenario

- Over 7,200 home users, companies, government agencies and law enforcement organizations were infected with Gozi, the data-stealing malware, by visiting infected web sites using IE browsers. Gozi, which silently downloads and executes on PCs, logs keystrokes to steal data, including bank and credit card account numbers. SSNs, online payment account numbers, and usernames and passwords, when the user visits a banking Web site or initiates an SSL session. Antivirus was not able to detect Gozi and its variants.



Cisco Solution

- IronPort S-Series protects against data-stealing malware by:
 - Protecting employees from access to malware-infected sites through the Web Reputation Filters.
 - Protecting infected PC's from sending private data by scanning all network traffic across every port to detect and block "phone-home" activity with the Layer 4 Traffic Monitor.
- Cisco Security Agent's behavior-based protection defends endpoints against all types of malware - malicious mobile code, rootkits, worms, and targeted attacks.

DLP Data-in-Motion

Data Loss through network remote access

Prevent data loss from unauthorized or unencrypted network remote access.

Scenario

- A vulnerability analysis at a major southern California hospital revealed that doctors were able to log into their hospital desktop computers from home via an Internet available RDP connection (no VPN) and were able to view patient information over an unencrypted channel.



Cisco Solution

- Cisco Adaptive Security Appliance supports SSL and IPsec VPNs to authenticate and encrypt communication channels for remote access users.
- Cisco Secure Desktop is available for use with Cisco SSL VPN to prevent data loss through:
 - Checking endpoint location / security posture before remote connections are established
 - Encrypting file downloads during a session
 - Providing post-session clean-up, e.g. deleting temporary files, internet history, and auto-complete p/w's
- Cisco NAC tightens the security policy by enforcing that all computers connected to the network via VPN are company-controlled computers and meet company's security policies.

DLP Data-in-Use

Data Loss through portable/removable media

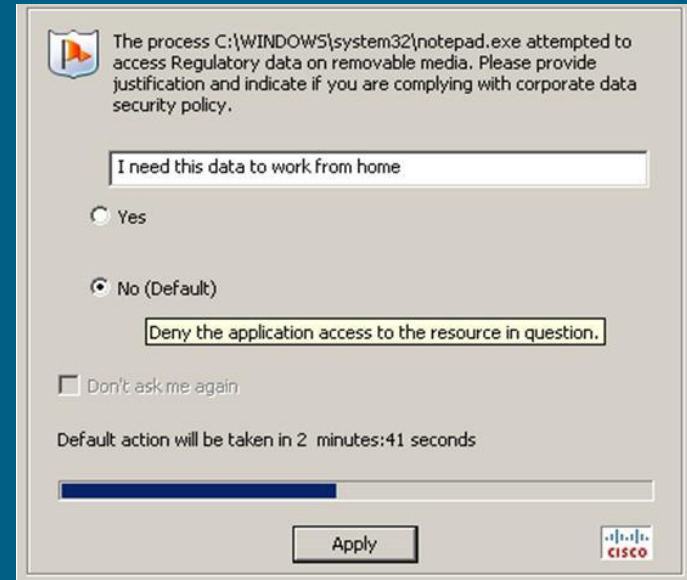
Prevent sensitive data from being transferred to removable media, such as thumb drives, USB sticks, or CD's.

Scenario

- Stockport Primary Care Trust (UK) reported a member of staff lost a USB memory stick containing data extracted from the medical records of 4000 patients. Data consisted of the NHS number, Stockport PCT identification number, first and second name, date of birth, sex, condition, GP code, practice code, and GP name.

Cisco Solution

- Cisco Security Agent can prevent files containing sensitive data or sensitive keywords from being copied to removable media, such as a USB stick.
- Cisco NAC can prevent unauthorized access to the network containing the sensitive databases.
- Cisco Trustsec can prevent unauthorized access to sensitive databases.



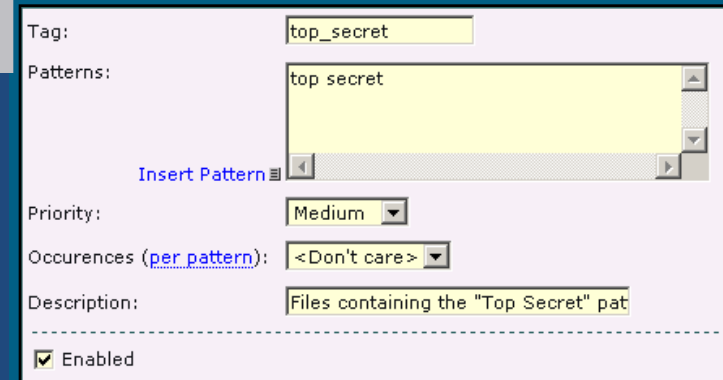
DLP Data-in-Use

Data loss through clipboard misuse

Prevent sensitive data from being copied and pasted to external-facing applications, such as blogs, social networking sites, or instant messaging.

Scenario

- Scenario HMO Kaiser Permanente informed 140 of their insureds that a former employee posted personal information such as names, addresses and telephone numbers, as well as medical record numbers and some routine lab information on her blog. Kaiser was one of the first to be fined for violating HIPAA by the California Department of Managed Health Care (DMHC).



The screenshot shows a configuration window for a Data Loss Prevention (DLP) rule. The fields are as follows:

- Tag:** top_secret
- Patterns:** top secret
- Insert Pattern:** (button)
- Priority:** Medium
- Occurrences (per pattern):** <Don't care>
- Description:** Files containing the "Top Secret" pat
- Enabled:** ☒

Cisco Solution

- Cisco Security Agent protects against Clipboard abuse, whether intentional or accidental, when sensitive data is cut, copied, pasted to an external Website (such as blogs or Facebook) or Instant Messenger.

DLP Data-at-Rest

Data loss through a File-Sharing Site

Prevent data loss from unauthorized access to a file sharing site.

Scenario

- Lexmark employee data was inadvertently exposed, including Social Security numbers, dates of birth, names and addresses, when it was accessed by two parties with unknown IP addresses. The employee data had been loaded to a file sharing site used to share information between business partners and Lexmark.



Cisco Solution

- Cisco Trust Sec integrates into your existing Cisco switching infrastructure to provide data loss protection through role-based identity access and control to critical or sensitive applications and resources, including file servers
- The Cisco ASA Firewall VPN service can restrict internal database access to specified business partners or internal employees.

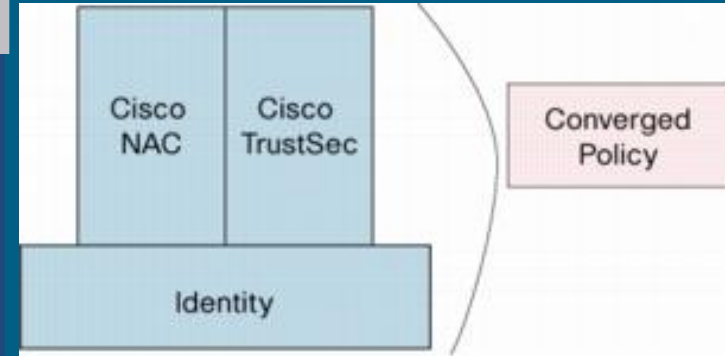
DLP Data-at-Rest

Unauthorized access to databases and back-end systems

Prevent databases or back-end systems from being accessed by unauthorized users, which can result in stolen private data or confidential information.

Scenario

- Jérôme Kerviel's ability to access systems he shouldn't have been able to led to the loss of \$8 billion in bad stock trades under French Bank Societe Generale. The a hit so large analysts claimed its ripple effects could be felt across the world's stock markets.



Cisco Solution

- Cisco Network Access Control controls and authorizes access to networks containing sensitive databases.
- Cisco Trustsec controls and authorizes access to systems containing sensitive data, from back-end databases and servers to mobile computers.
- Cisco Security Agent can prevent access to sensitive files located on restricted databases.

DLP Data-at-Rest

Data loss through lost storage devices

Prevent data loss from lost or stolen tapes or storage devices by encrypting sensitive information.

Scenario

- Iron Mountain lost a backup tape belonging to GE Money that contained credit card information from approximately 650,000 customers. The unencrypted tape also held Social Security numbers for 150,000 customers. J.C. Penney was among the 230 retailers were affected by the breach. GE Money is reportedly paying for a year of credit monitoring service to help protect those whose social security numbers were on the tape from identity theft.



Cisco Solution

Cisco Storage Media Encryption

- Provides a secure solution for encrypting data at rest on heterogeneous, SAN attached tape devices and virtual tape libraries (secure AES-256)
- Integrates into your existing Cisco switching infrastructure, such as Cisco MDS 9000 Series Multilayer Switches

DLP Data-at-Rest

Data loss through Web applications

Prevent data loss from unauthorized access to web applications.

Scenario

- Linden Lab discovered that a hacker accessed its Second Life database through web servers. The affected data included unencrypted account names, real life names, contact information, encrypted account passwords, and payment information.



Cisco Solution

- Cisco ACE Web Application Firewall
 - Protects against Web-based attacks, such as cross-site scripting (XSS) attacks or SQL and command injection, which are often designed to intercept or steal credit card information via Web applications.
 - Protects from the loss of sensitive data, such as credit cards, passport numbers, or social security numbers by monitoring and filtering outbound traffic.

Compliance Regulations

Data-at-rest, data-in-motion, data-in-use

Compliance regulations such as PCI, HIPAA and SoX require data protection all the time

Scenario

- Over 100,000 compliance regulations world wide, most of them focused on protecting some type of data from lost, theft or tampering
- Data breach laws in the United States force companies to disclose data loss. Data breach laws are expanding to other countries



Cisco Solution

- Cisco Self-Defending Network
 - automatically and dynamically protects data from being lost through the layered defense
 - Protects from the loss of sensitive data, such as credit cards, medical information, social security numbers or financial information by monitoring and filtering access to the data while at rest, through email and data in-use, and while data is in motion both inbound and outbound.

Conclusions



Cisco Expo
2009

Welcome to the Human Network.



Recommendations for 2009

- Stay focused –prioritize strategically
- Stop users from downloading malware onto the network
- Fix existing vulnerabilities
- Prevent data loss
- Take insider threats seriously
- Think beyond compliance
- Make security simpler



Observations

“Our research presents an opportunity to evolve security toward a much-needed combination of education, policy, and technology.”

John N. Stewart, Chief Security Officer, Cisco

Recommendations

- Identify data that needs to be protected
- Don't assume employees know what data to protect
- Keep in touch with employees, understand their jobs
- Provide security education everywhere
- Integrate all corporate entities into same security culture



Data Loss Prevention Summary

- There is no Silver Bullet to Security, including Data Loss Prevention
- With a Self-Defending Network as a foundation and integrated DLP into security devices, organizations can better:
 - Prevent data loss, including intellectual property and customer/employee private data
 - Enforce regulatory and acceptable use policies
 - Increase visibility into sensitive data usage
 - Decrease cost and complexity of DLP deployments
 - Protect data in motion, in use, and at rest



Q & A



Cisco Expo
2009

Welcome to the Human Network.

