



Safe & Secure Environments for School



Ricky Elias

Security Architect

Advanced Technologies (Security)

relias@cisco.com

Agenda

▶ Current Challenges

▶ Cisco Solutions

▶ Case Studies

▶ Q and A



Online Security: A Story in Two Parts

- Outside coming in
 - Probing
 - Viruses
 - Attacks on student resources
 - ...
- Inside going out
 - What students and visitors bring to schools
 - DDoS launching code and

From Fame to Monetary Gain

Jeanson James Ancheta



Downey, Calif., Police

BUT instead of setting up a website to request permission to install ads — a common practice — he used his bots to install adware on connected PCs, court records show. Each piece of adware installed raked in a few cents.

Working at home, Ancheta nurtured the botnet during a workday that usually began at 9 a.m. and stretched non-stop until 5 a.m., a court document said. He hired an attorney to help with the case. He hired an attorney to help with the case.

- Hijacked more than 400,000 PCs, used them to build a botnet, then rented out the system to spyware distributors, hackers, and spammers
- Made \$3,000 from renting the botnet to others, who used it to launch denial-of-service (DoS) attacks and spew spam
- Pocketed an additional \$107,000 by seeding the botnet's PCs with adware and raking in affiliate fees
- Pleaded guilty to federal charges, sentenced to 57 months

“Installs” for Sale — Monetizing Botnets

The image shows a screenshot of a web browser displaying an article on the Dark Reading website. The article is titled "Schools Suffer One-Third of Total U.S. Data Breaches" and is dated November 13, 2008. The author is Kelly Jackson Higgins. The article's content states that a new report reveals that 12.4 million student and consumer profiles were compromised in 324 breaches at colleges and K-12 schools. The website's navigation menu includes categories such as "ATTACKS / BREACHES", "VULNERABILITIES", "APPLICATION S", "SECURITY MANAGEMENT", "STORAGE SECURITY", and "ENCRYPTIO". The page number "5" is visible at the bottom right, and the word "Asia" is at the bottom left.

SOTONA

SECURITY
darkREADING

ATTACKS / BREACHES | VULNERABILITIES | APPLICATION S
SECURITY MANAGEMENT | STORAGE SECURITY | ENCRYPTIO

Sec
June 2009
Camp
Alleged p
Dennis Carter
Assistant Editor
Two Missouri b
by a federal grand
gally harvesting st
from more than 2

SCHOOL NEWS
neme
students
fice
that
, in-
sity
orks

Schools Suffer One-Third of Total U.S. Data Breaches

New report reveals 12.4 million student and consumer profiles were compromised in 324 breaches at colleges, K-12 schools

Nov 13, 2008 | 05:11 PM

By Kelly Jackson Higgins
DarkReading

Asia 5

Cisco Education Solution Portfolios

Administrative Efficiency

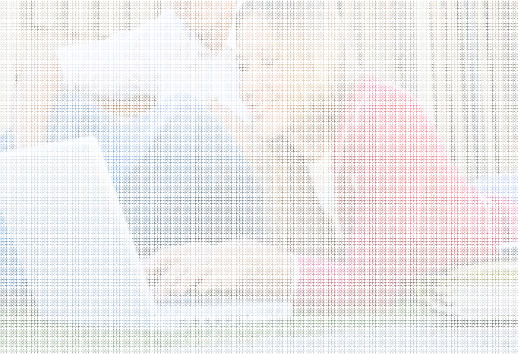
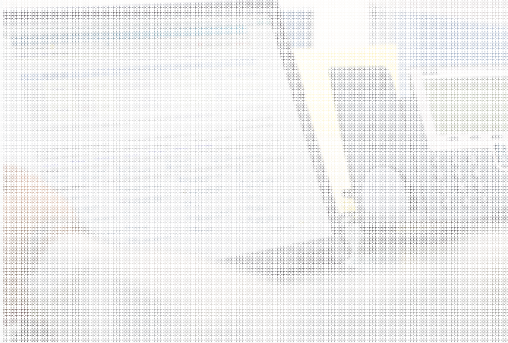
- Unified Communications
- Education in Motion
- Digital Media System
- Connected Real Estate
- Data Center

Safe & Secure Environments for Education

- Provide enforcement and accountability
- Secure the web and school network
- Protect critical resources and data

Next-Generation Learning

- Unified Communications
- Education in Motion
- Digital Media System
- Virtual Classroom
- TelePresence
- High-Performance Computing



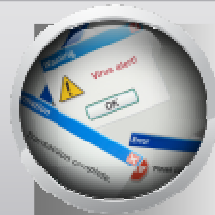
Layered Security

Security Needs



Student records and personal data

Protect critical resources and data



Safe online learning environment

Secure the web and school network



Policy and control

Provide enforcement and accountability

Goals

Technologies

- Firewall
- Web security
- Network admission control

Provide Enforcement & Accountability

Cisco Network Admission Control (NAC) for Education

Keeping Schools Safe and Secure

- Secure access to school network
- Protect against viruses and other network infections
- Prevent unauthorized access to personal data and academic records
- Assist in compliance with regulatory requirements



Secure School Network



List of Roles	New Role	Traffic Control	Bandwidth	
Role Name	IPSec	Roam	VLAN	Description
Unauthenticated Role	deny	deny		Role for unauthenticated users
Temporary Role	deny	deny		Role for users to download requirements
Quarantine Role	deny	deny		Role for quarantined users
Allow All	deny	deny		Full Access
Guest Access	deny	deny	:666	guest privileges
consultant access	deny	deny	:55	consultant privileges

Prevent Network Infections



Cisco NAC Web Agent

 Cisco NAC Web Agent

Host is not compliant with network security policy

Your device does not conform to the required security policies for this protected network. Your access to the network is refused or limited until you are able to comply with the security requirements listed below.
Please remediate by 12:57:59 AM, Fri Oct 05, 2007.

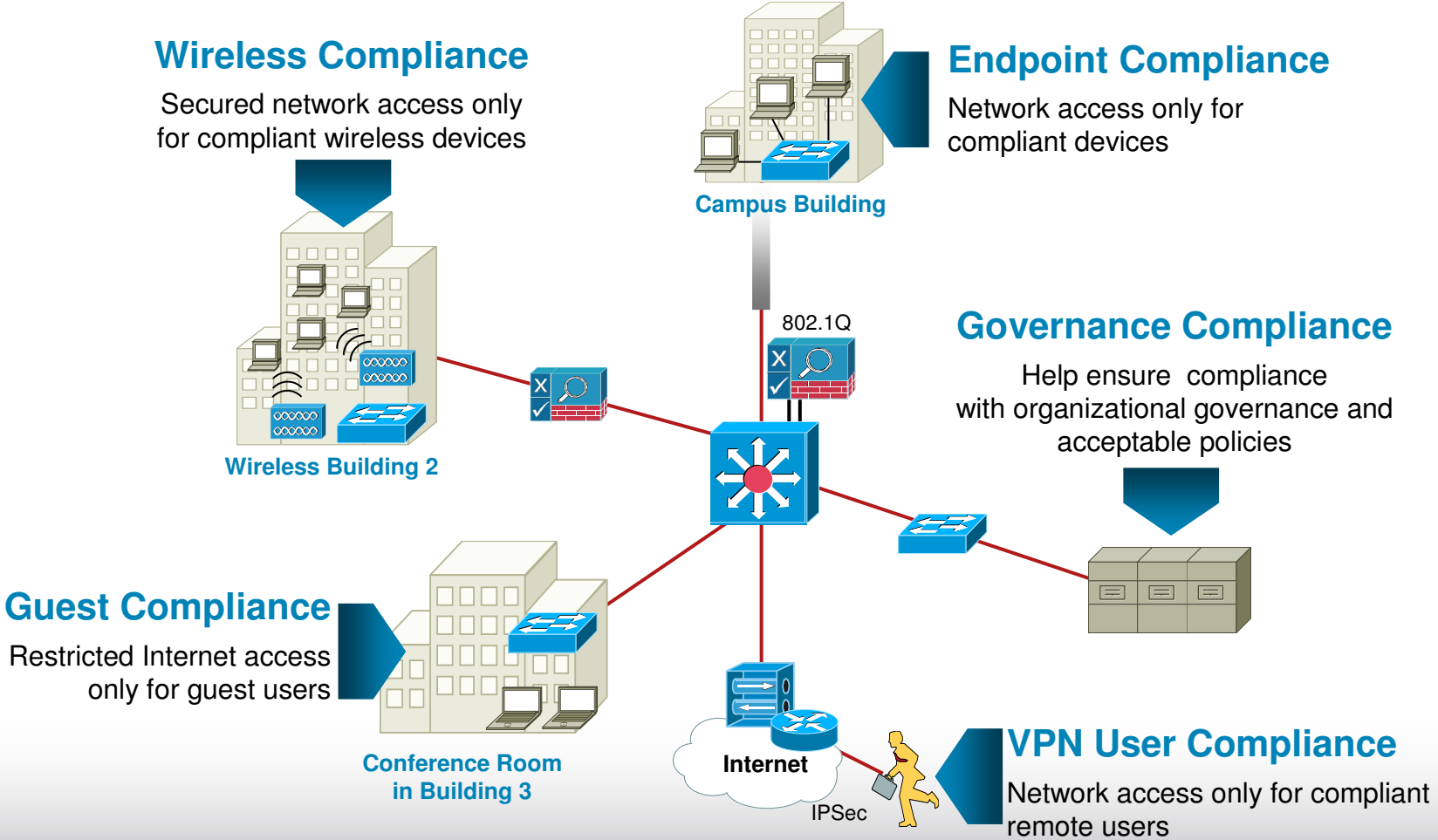
Security Compliance Summary

Result	Security Requirement	Remediation Suggestion
	McAfee-AV-Running	McAfee AV needs to be turned ON.
	CorporateAssetCheck	Only Corporate Assets Allowed
	McAfee AV Check	

Cisco NAC Web Agent Version 4.1.3.1 - Report Generated 12:43:00 AM, Fri Oct 05, 2007

00:14:35 Remaining

Meeting Student and Faculty Needs



Network Admission Control Benefit

Cisco NAC Benefits

Schools Gain

Threat containment

- Fewer infections
- Reduced interruptions to education
- More resilient school network

Access control

- Decline in incidents
- Less loss of personal data and school records

Compliance

- Improved security
- More reliable audit and enforcement

Case Study: Virginia Commonwealth University

Protect Students, Faculty and Staff

Situation / Challenge

- Balance need for academic openness with need to protect information and assets
- Government laws/regulations and industry requirements to be met

Solution/

- Provide secure online access while thwarting threats
- Implement a campus network access and enforcement policy to minimize incident and virus outbreaks
- Retain logs, audit/tracking information, and reports to meet compliance requirements, and demonstrate compliance with P2P/RIAA regulations
- Video monitor school events, and validate students with their own RFID cards as they enter the site

Technology

- Cisco Security Solutions, Cisco Network Admission Control (NAC) Profiler, Cisco NAC Guest Server, Cisco Physical Access Control, Cisco Video Surveillance Manager

“Since the Cisco NAC solution has been in place, we have seen an approximately 90 percent drop in infections on the student resident network.”

— Jesse Crim, Information Security Analyst, Virginia Commonwealth University

Secure the Web and School Network

Cisco IronPort Web Security Appliance (WSA) for Education

Protecting Students from Harmful Content

- Secure and control access to the Internet
- Protect against malware, spyware, and zero-day threats
- Enforce acceptable-use policies for Internet use, including role-based administration and access



Cisco IronPort WSA Protects School Users



Layer 4 Traffic Monitor

Web Reputation Filters

Dynamic Vectoring and Streaming Engine

- Detects malicious botnet traffic across all ports

- Blocks 70% of known and unknown malware traffic at connection time

- Blocks malware based on deep content analysis



Detect Existing Client Infections

Threat Spotlight – Gozi Trojan Exploit

- Trojan program designed to steal data from encrypted Secure Sockets Layer (SSL) stream.
- Undetected for more than 50 days has stolen more than **10,000 records** containing confidential information.
 - 2,000 SSN, account numbers, usernames/ passwords tied bank accounts and retail/ e-commerce sites.
 - The black market street value of the stolen data: \$2 million.
- Took advantage of a vulnerability in the iFrame tags of Microsoft Corp.'s Internet Explorer

The screenshot shows a news article from IT Week. The article title is "Smart malware steals from SSL streams" by Iain Thomson, dated 22 May 2007. The article text includes "Is nothing safe?" and "A new variant of the malware is stealing data". The article is part of a "Hacking" news section. The page also features a sidebar with navigation links and a "MORE RELATED CONTENT" section.

Respond now for your free guide to faster WEB application delivery. CITRIX

100 BEST PLACES TO WORK IN IT 2007 VIEW NOW

COMPUTERWORLD Security IDG

JUMP TO More Resources SEARCH Google™ Custom Search

Home News E-mail Newsletters Tech Dispenser Shark Bait Knowledge Centers Operating Systems Networking & Internet Mobile & Wireless Security

IT Week > News > Hacking

Smart malware steals from SSL streams

Is nothing safe?

Iain Thomson, vnunet.com, 22 May 2007

A new variant of the malware is stealing data

Hackers use 'construction kit' to unleash Trojan variants

The Trojans have already stolen sensitive data from 10,000 people

Jaikumar Vijayan Today's Top Stories or Other Security Stories

Comments (1) Recommendations: 92 — Recommend this article

June 25, 2007 (Computerworld) -- Multiple hacker groups are using a "construction kit" supplied by the author of a Trojan horse program discovered last October to develop and unleash more dangerous variants of the original malware.

MORE RELATED CONTENT

- Infected job-search sites info-theft for 46,000

Acceptable Internet Use Policy

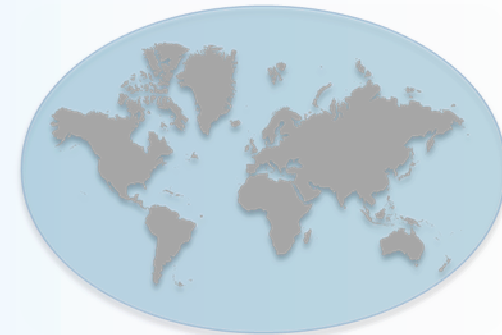
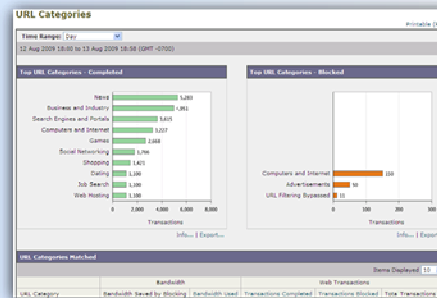
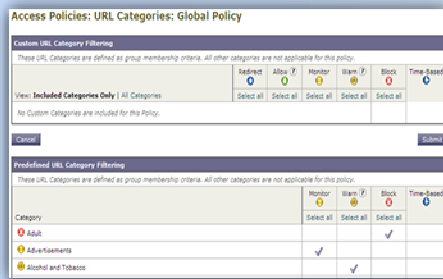
Example

Prohibited uses and activities include, without limitation, any use of the Services in a manner that involves, facilitates, or attempts any of the following:

- gambling activities;
- displaying, performing, sending, receiving or storing any content that is obscene, pornographic, lewd, lascivious, or excessively violent, regardless of whether the material or its dissemination is unlawful;
- advocating or encouraging violence against any government, organization, group, individual or property, or providing instruction, information, or assistance in causing or carrying out such violence, regardless of whether such activity is unlawful;
- accessing, sending, receiving, displaying, performing, disclosing, storing, or executing any content a) in violation of any copyright, right of publicity, patent, trademark, service mark, trade name, trade secret or other intellectual property right, b) in violation of any applicable agreement, or c) without authorization

Cisco IronPort Web Usage Controls

Leading Efficacy, Rich Controls, Comprehensive Visibility



Control

- Per user, per group policies
- Multiple actions: block, warn, monitor
- Time-based policies
- Unlimited custom categories
- Custom end-user notifications

Visibility

- Easy to understand reports
- Extensive logging
- Comprehensive alerting

Efficacy

- 200+ countries
- 50+ languages
- 65 categories
- Less than 1 in 1 million false positives

Case Study: Enumclaw School District

■ Enumclaw School District's challenge:

- 5 elementary schools, 2 middle schools, 1 high schools
- Ensure students, teachers and administrators make the most of its computing technology – while receiving only appropriate Internet content
- Previous filtering solution provided inadequate integration with user directories,



If there's an identified threat, it's blocked at the gateway – rather than on the desktop after the threat is already inside the network.

The ability to dynamically block webpages is very powerful. This is something we were not able to do previously. The Cisco IronPort S160 is like a firewall for web traffic.

■ IronPort's solution:

Since deploying the Cisco IronPort S160, the district reports a daily average of:

- 200 suspicious URLs blocked by Cisco IronPort Web Reputation Filters
- 45,500 URLs stopped by Cisco IronPort URL Filters
- At least 10 malware or spyware downloads blocked

Chad Marlow
Technology Coordinator
Enumclaw School District

USERS
PROTECTED

4000+

Protect Critical Resources and Data

Cisco Adaptive Security Appliance (ASA) for Education

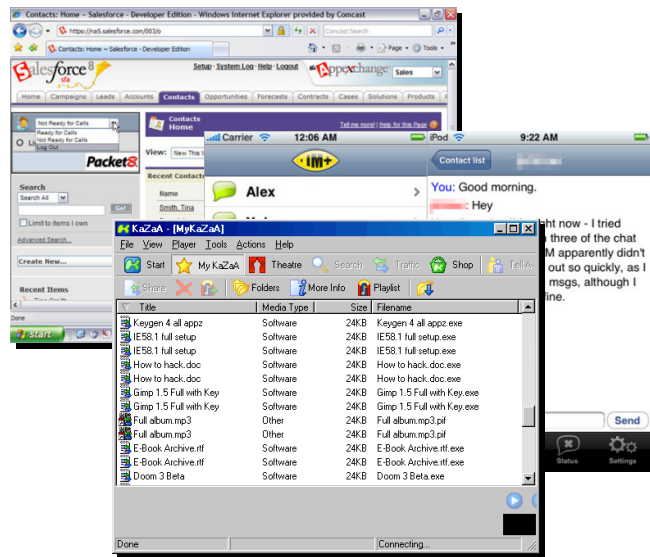
Supporting 21st-Century Education

- Provides strong protection for the network by quickly detecting and responding to threats and risks
- Keeps sensitive and confidential information safe and prevents financial loss due to data breach or leakage
- Guards valuable assets and intellectual properties
- Prevents unauthorized access to certain website classifications
- Assists in compliance with regulatory requirements



Application and User-Centric Security

Access Control for Modern Networks



Application Access Control

- Integrated HTTP & Port 80
- IM & P2P
- Content type & Active-X



Authentication Policies

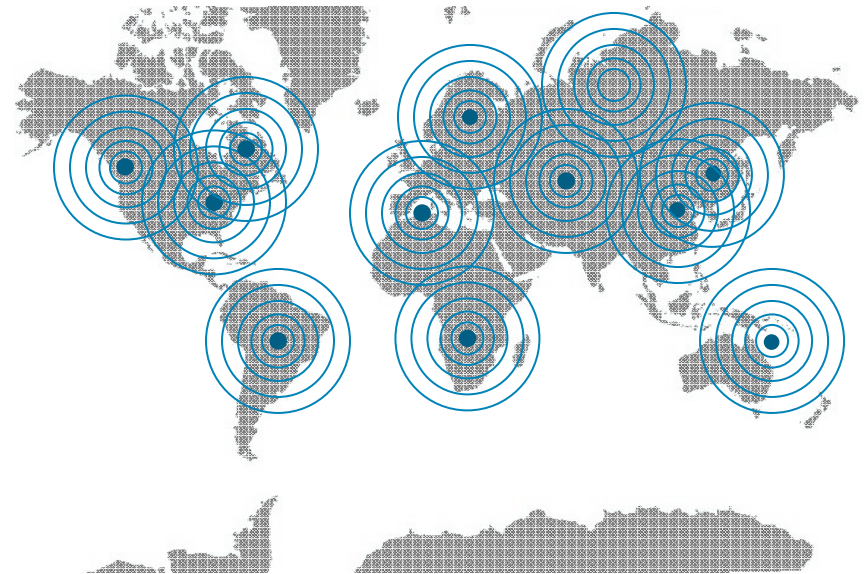
- Selective access to assets
- Track and audit user activity
- Extensive protocol support

Global Correlation in Action

Network IPS to Global IPS

08:00 GMT

- A sensor in Australia detects new malware
- A sensor in Russia detects a botnet issuing new commands
- A sensor in Korea detects a virus mutating
- A sensor in Florida detects a hacker probing major financial institutions



08:15 GMT

- All Cisco IPS customers protected

Responsive and Accurate
Protection

Detecting Client Infections

Botnet Traffic Filters

Cisco ASDM 6.2 for ASA - Demo mode

File View Tools Wizards Window Help Look For: Go

Home Configuration **Monitoring** Save Refresh Back Forward Help

Monitoring > Botnet Traffic Filter > Reports

Reports

Top Botnet Sites

Botnet Site	Connections
66.40.9.250 (data.ale...)	515
209.10.2.3 (cdn5.tribalfusion...)	291
209.100.1.100	159
64.123.21.11	94
44.23.22.11 (cgi.alexa.com)	80
63.11.34.123 (ieplugin.com)	62
208.11.222.11 (l1.zedo.com)	61
209.123.100.3	59
208.111.123.11 (pay-per-search.com)	54
66.111.2.3 (context3.kanoodl...)	49

IP Address	Botnet Site	Connections
66.40.9.250	data.alexa.com	515
209.10.2.3	cdn5.tribalfusion...	291
209.100.1.100		159
64.123.21.11		94
44.23.22.11	cgi.alexa.com	80
63.11.34.123	ieplugin.com	62
208.11.222.11	l1.zedo.com	61
209.123.100.3		59
208.111.123.11	pay-per-search.com	54
66.111.2.3	context3.kanoodl...	49

Whois
Save as PDF
Clear Report

Top Botnet Ports

Botnet Port	Connections
tcp 1000	617
tcp 2001	472
tcp 23	22
tcp 1001	19
udp 2000	17
udp 2001	17
tcp 8080	9
tcp 80	3
tcp >8192	2

Botnet Port	Connections
tcp 1000	617
tcp 2001	472
tcp 23	22
tcp 1001	19
udp 2000	17
udp 2001	17
tcp 8080	9
tcp 80	3
tcp >8192	2

Save as PDF
Clear Report

Refresh

Last Updated: 2/24/09 8:51:45 AM

Data Refreshed Successfully. <admin> 15 3/16/07 11:09:41 AM PDT

Cisco Solutions for Information Security

Protect Data and Prevent Attacks



Features

- Identity-based network security
- Cisco Campus Secure protects wired and wireless networks and endpoints
- Cisco Network Security is embedded in all solutions
- Cisco ASA 5500 Series Adaptive Security Appliances



Benefits

- Prevent cyber attacks
- Keep records safe
- Protect students from harmful online sites or predators
- Monitor bandwidth

Indiana State University enables automated bandwidth control



Cisco's Commitment to Higher Education

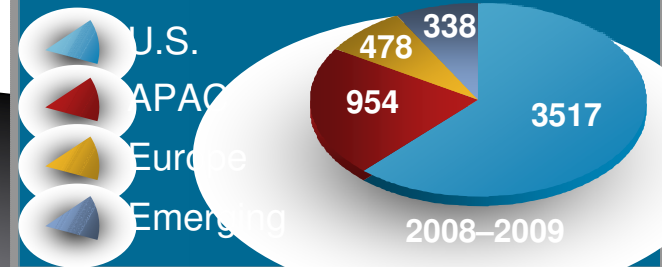
Internet and Education: The two great equalizers

IBSG Higher Education

- Thought Leadership
- Strategy
- Innovation
- Models



University Recruitment/Interns



Cisco Research Center

- Funded Research
- Collaboration Projects
- Technology Transfer



Cisco Networking Academy

- 9000+ Academies
- 760,000+ Students Per Year
- 160+ Countries





CISCO