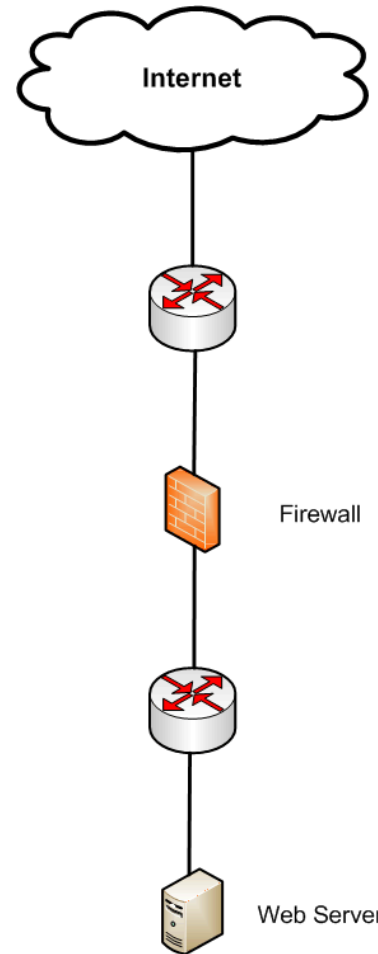




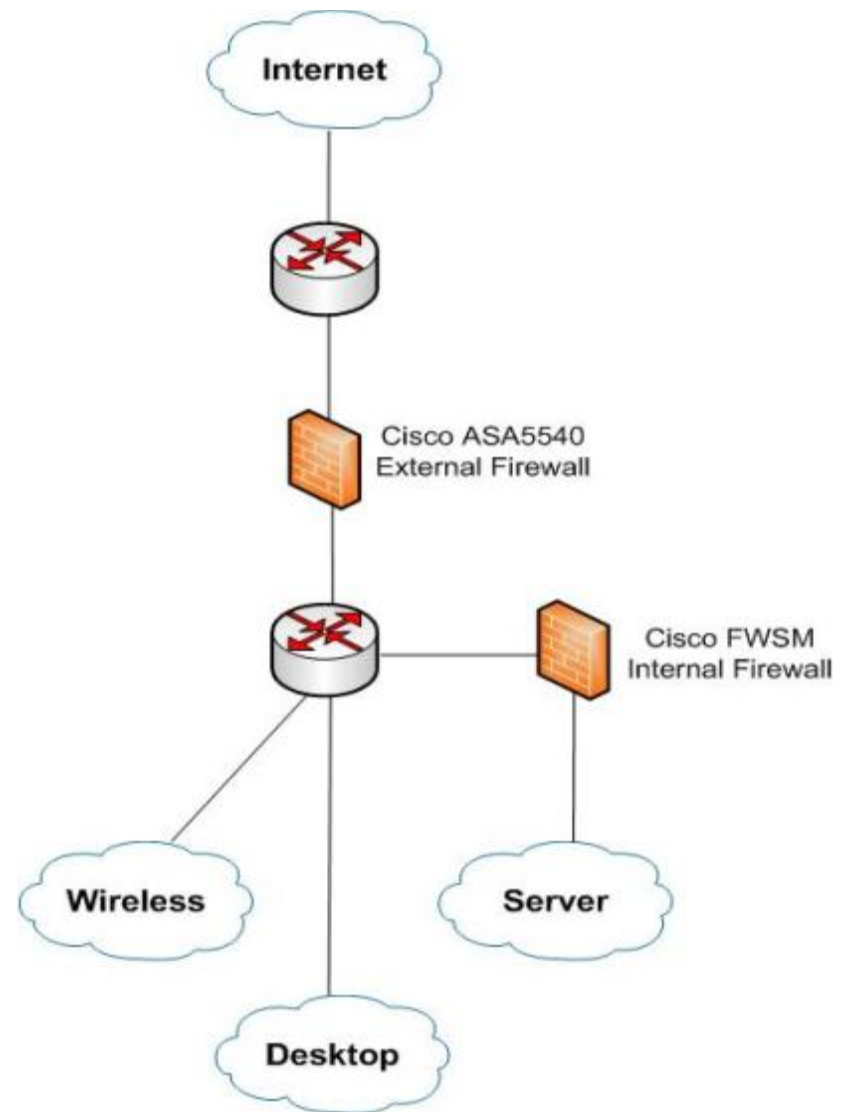
Technology Security >>

# Firewall



# Firewall deployment

- ▶ Macomb
  - Campus – ASA5540
  - ResNet – ASA5540
  - Servers – FWSM
- ▶ QCC
  - 60<sup>th</sup> St – ASA5520
  - Caxton – ASA5510
  - WQPT – ASA5505
  - Arsenal – ASA5505
    - Not installed yet
    - ETA: April 20, 2011



# Daily Firewall Counts

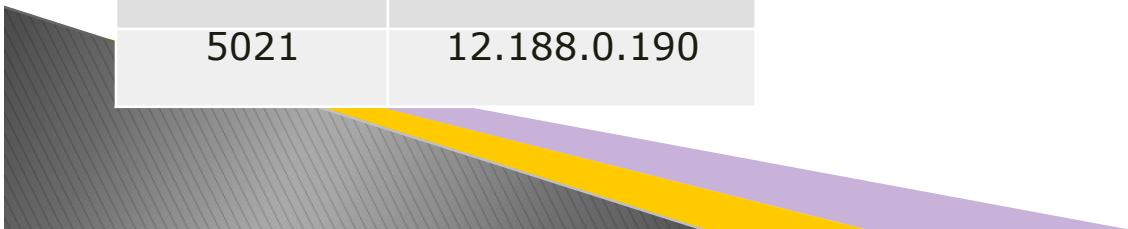
	Average per day
Macomb ASA & FWSM	11,401,986
QCC (60 <sup>th</sup> St, WQPT, Caxton)	222,903
Total	11,624,889

We deny approximately 4.2 billion attempted connections per year.















# Top 12 Source Connections






Count	IP
31479	96.9.147.197
28130	60.173.26.55
26683	58.216.238.252
12939	221.1.220.185
9147	61.47.10.231
6845	211.214.160.120
6792	85.105.23.83
6513	174.90.21.156
5797	221.185.163.208
5399	66.151.128.210
5234	173.15.68.193
5021	12.188.0.190



# Top 12 Source Connections

Count	IP	Location
31479	96.9.147.197	Pennsylvania, USA 
28130	60.173.26.55	China 
26683	58.216.238.252	China 
12939	221.1.220.185	China 
9147	61.47.10.231	Thailand 
6845	211.214.160.120	Republic of Korea 
6792	85.105.23.83	Turkey 
6513	174.90.21.156	Canada 
5797	221.185.163.208	Japan 
5399	66.151.128.210	California, USA 
5234	173.15.68.193	Comcast, USA 
5021	12.188.0.190	Macomb, IL 

# Top 12 Source Connections

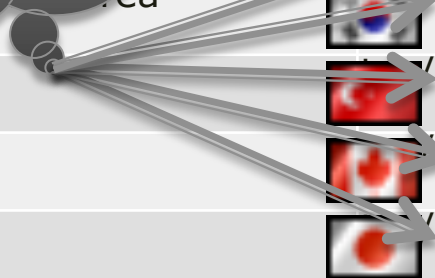
Count	IP	Location		Protocol/port
31479	96.9.147.197	Pennsylvania, USA		tcp/2967 (ssc-agent)
28130	60.173.26.55	China		tcp/3306 (my-sql)
26683	58.216.238.252	China		tcp/27977
12939	221.1.220.185	China		tcp/1022 (exp2)
9147	61.47.10.231	Thailand		tcp/445 (microsoft-ds)
6845	211.214.160.120	Republic of Korea		tcp/445 (microsoft-ds)
6792	85.105.23.83	Turkey		tcp/445 (microsoft-ds)
6513	174.90.21.156	Canada		tcp/445 (microsoft-ds)
5797	221.185.163.208	Japan		tcp/445 (microsoft-ds)
5399	66.151.128.210	California, USA		icmp (ping)
5234	173.15.68.193	Comcast, USA		udp/53 (DNS)
5021	12.188.0.190	Macomb, IL		udp/53 (DNS)

# Top 12 Source Connections

Count	IP	Location	Port
31479	96.9.147.197	Pennsylvania, USA	3306 (mysql)
28130	60.173.26.55	China	3306 (mysql)
26683	58.216.238.255	China	27977
12939	221.1.220.1	China	1022 (exp2)
9147	61.47.10.2	China	445 (microsoft-ds)
6845	211.214.160.120	Kenya	445 (microsoft-ds)
6792	85.105.23.83	Turkey	445 (microsoft-ds)
6513	174.90.21.156	Canada	445 (microsoft-ds)
5797	221.185.163.208	Japan	445 (microsoft-ds)
5399	66.151.128.210	California, USA	80 (http)
5234	173.15.68.193	Comcast, USA	53 (DNS)
5021	12.188.0.190	Macomb, IL	53 (DNS)

SQL port used by databases


Microsoft SMB ports used for file sharing





# Top 12 Destinations

Count	IP
100203	143.43.179.15
88494	143.43.186.135
63998	143.43.184.245
22358	143.43.213.114
20180	143.43.142.11
19106	143.43.178.150
18458	143.43.156.122
17384	143.43.189.2
16545	143.43.191.157
15723	143.43.188.182
14375	143.43.190.131
13074	143.43.188.241



# Top 12 Destinations

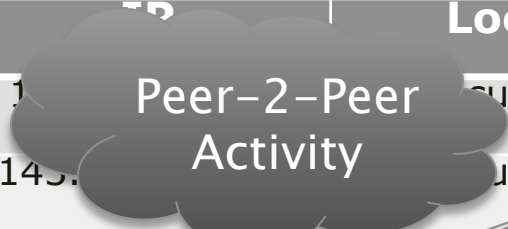
Count	IP	Location
100203	143.43.179.15	Non-secure Wireless
88494	143.43.186.135	Non-secure Wireless
63998	143.43.184.245	Non-secure Wireless
22358	143.43.213.114	Brophy
20180	143.43.142.11	DNS server
19106	143.43.178.150	Non-secure Wireless
18458	143.43.156.122	Not used
17384	143.43.189.2	Non-secure Wireless
16545	143.43.191.157	Non-secure Wireless
15723	143.43.188.182	Non-secure Wireless
14375	143.43.190.131	Non-secure Wireless
13074	143.43.188.241	Non-secure Wireless

# Top 12 Destinations

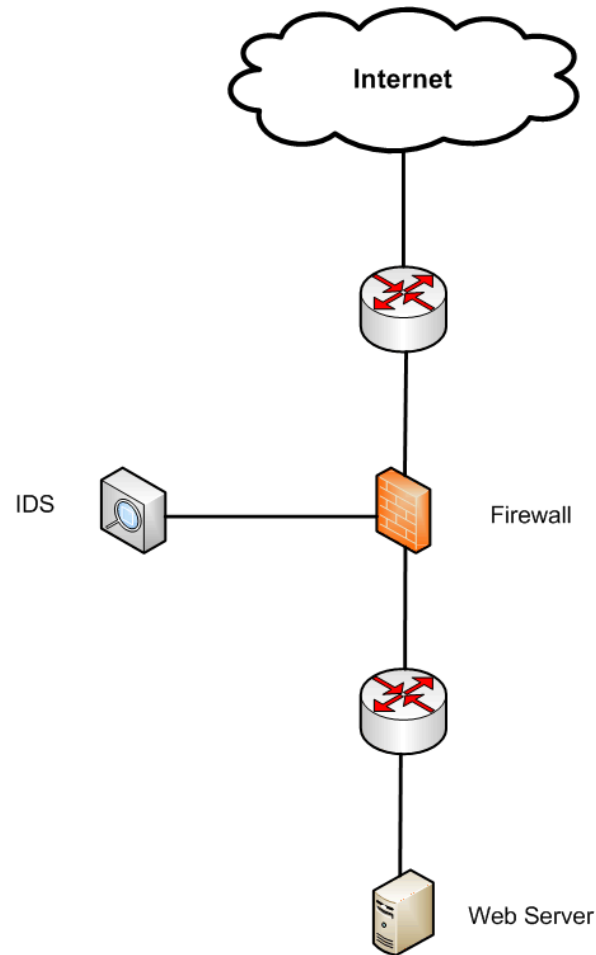
Count	IP	Location	Protocol/port
100203	143.43.179.15	Non-secure Wireless	misc protocols (tcp, udp, icmp)
88494	143.43.186.135	Non-secure Wireless	icmp
63998	143.43.184.245	Non-secure Wireless	udp/22864
22358	143.43.213.114	Brophy	udp/8889
20180	143.43.142.11	DNS server	icmp, udp/53 (DNS)
19106	143.43.178.150	Non-secure Wireless	misc protocols (tcp, udp, icmp)
18458	143.43.156.122	Not used	misc udp ports
17384	143.43.189.2	Non-secure Wireless	udp/24844
16545	143.43.191.157	Non-secure Wireless	misc protocols (tcp, udp, icmp)
15723	143.43.188.182	Non-secure Wireless	udp/40089 tcp/40089
14375	143.43.190.131	Non-secure Wireless	udp/37981
13074	143.43.188.241	Non-secure Wireless	udp/55381

# Top 12 Destinations

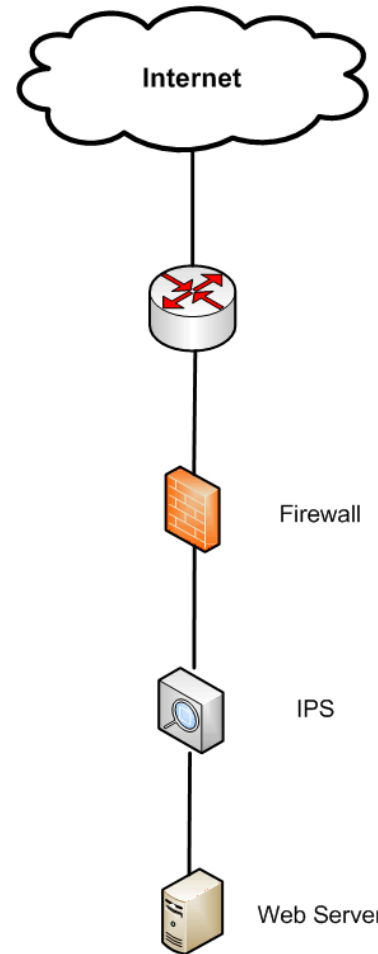
Count	IP	Location	Protocol/port
100203	143.43.188.241	Peer-2-Peer Activity	misc protocols (tcp, udp, icmp)
88494	143.43.188.241	Peer-2-Peer Activity	icmp
63998	143.43.184.245	Non-secure Wireless	udp/22864
22358	143.43.213.114	Brophy	udp/8889
20180	143.43.142.11	DNS server	icmp, udp/53 (DNS)
19106	143.43.178.150	Non-secure Wireless	misc protocols (tcp, udp, icmp)
18458	143.43.156.122	Not used	misc udp ports
17384	143.43.189.2	Non-secure Wireless	udp/24844
16545	143.43.191.157	Non-secure Wireless	misc protocols (tcp, udp, icmp)
15723	143.43.188.182	Non-secure Wireless	udp, 40089 tcp/40089
14375	143.43.190.131	Non-secure Wireless	udp, 37981
13074	143.43.188.241	Non-secure Wireless	udp/55381



# Intrusion Detection System(IDS)



# Intrusion Prevention System (IPS)



# IDS/IPS types

## ▶ Signature

- Uses list of signatures to detect bad traffic, similar to Anti-Virus software
- Pros
  - Proven technology
  - Very few false positives
- Cons
  - Only as good as signatures
  - Cannot detect 0-day

## ▶ Statistical anomaly (Heuristics)

- Notices changes in network behavior
- Pros
  - Can detect 0 day
- Cons
  - Newer technology
  - Large database
  - Does not work well when traffic changes

# IDS/IPS used at WIU

## ▶ Cisco SSM

- Signature based IPS
- Installed inside the Cisco ASA's, sees all Internet traffic
  - Macomb Campus
  - QC 60<sup>th</sup> St
  - QC WQPT
  - QC Caxton

## ▶ Stealth Watch

- Heuristics based IDS
- Monitors all of Macomb campuses network core traffic, sees all Internet and Server traffic





# Daily IPS Alerts Denied – Cisco SSM

	Total Alerts	Denied Alerts
All alerts	268,158	159,609
High alerts	2,195	1,999

We deny approximately 729 thousand high level attacks a year.



# Quality of Service (QOS)

- ▶ Used to control bandwidth
- ▶ Reserves bandwidth for mission critical services
- ▶ Makes sure that all other devices get an equal amount of bandwidth
- ▶ Packeteer
  - Macomb campus
  - QC 60<sup>th</sup> St campus

# Packeteer Implementation

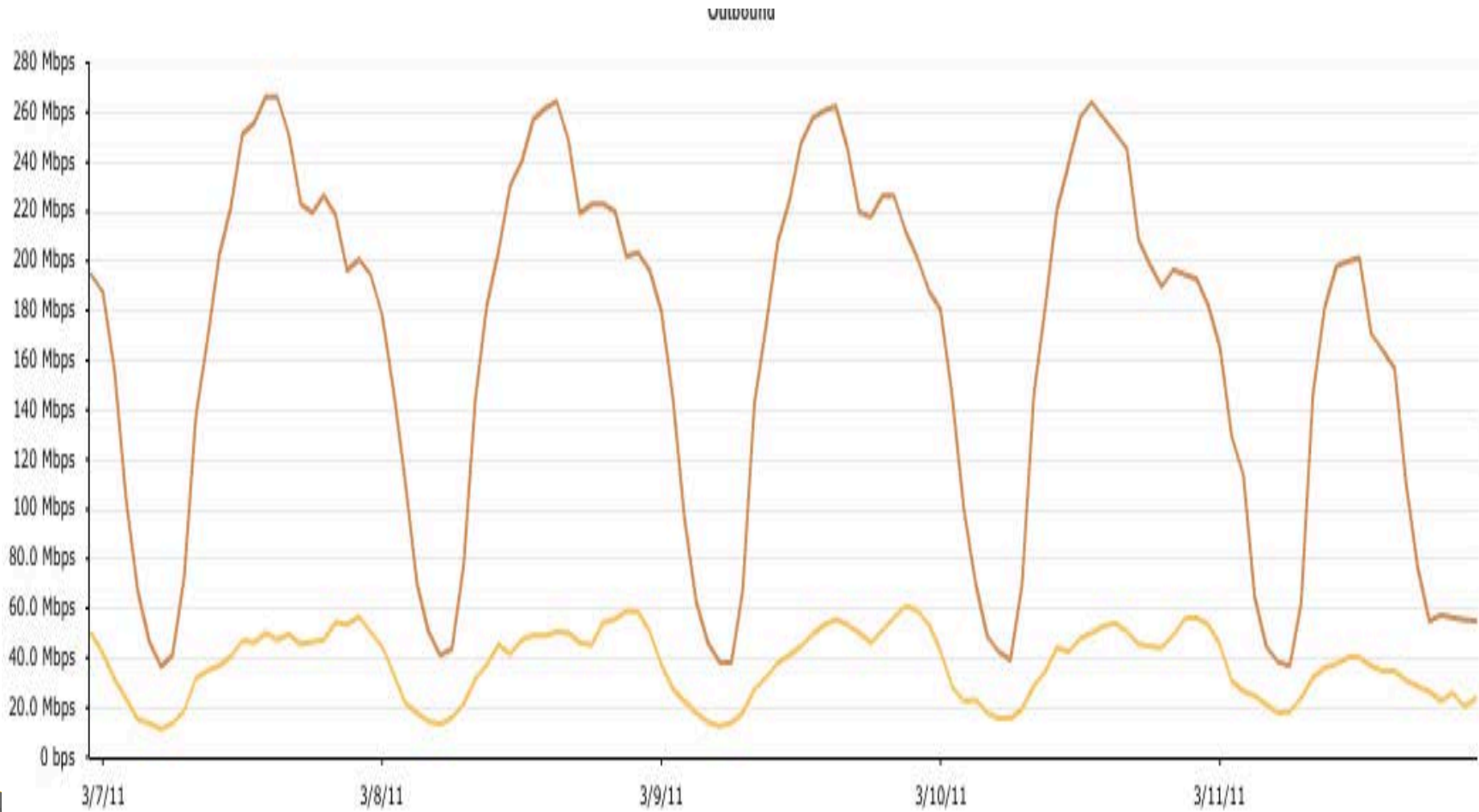
- ▶ Peer-2-peer
  - All P2P is limited to 2MB container.
- ▶ Exceptions
  - All mission critical services are placed in this partition, i.e. Zimbra, western online, web servers...
  - This allows these services to have some bandwidth reserved.
- ▶ Dynamic Partitions
  - Default container.
  - Automatically adjust bandwidth so all users get a fair amount.

# Packeteer – Dynamic Partitions

- ▶ Macomb – 2Mbps
- ▶ ResNet – 1 Mbps
- ▶ QC-60<sup>th</sup> St. – 3Mbps



# Packeteer – Macomb Campus



# Virtual Private Network (VPN)

- ▶ Used to allow secure access to our trusted intranet from the un-trusted Internet
- ▶ Macomb
  - Two Cisco ASA-5520's for redundancy
  - QCC – The main firewall is also doing VPN
- ▶ We implement our VPN in three different classifications
  - Site to site
  - Vendors
  - Clients

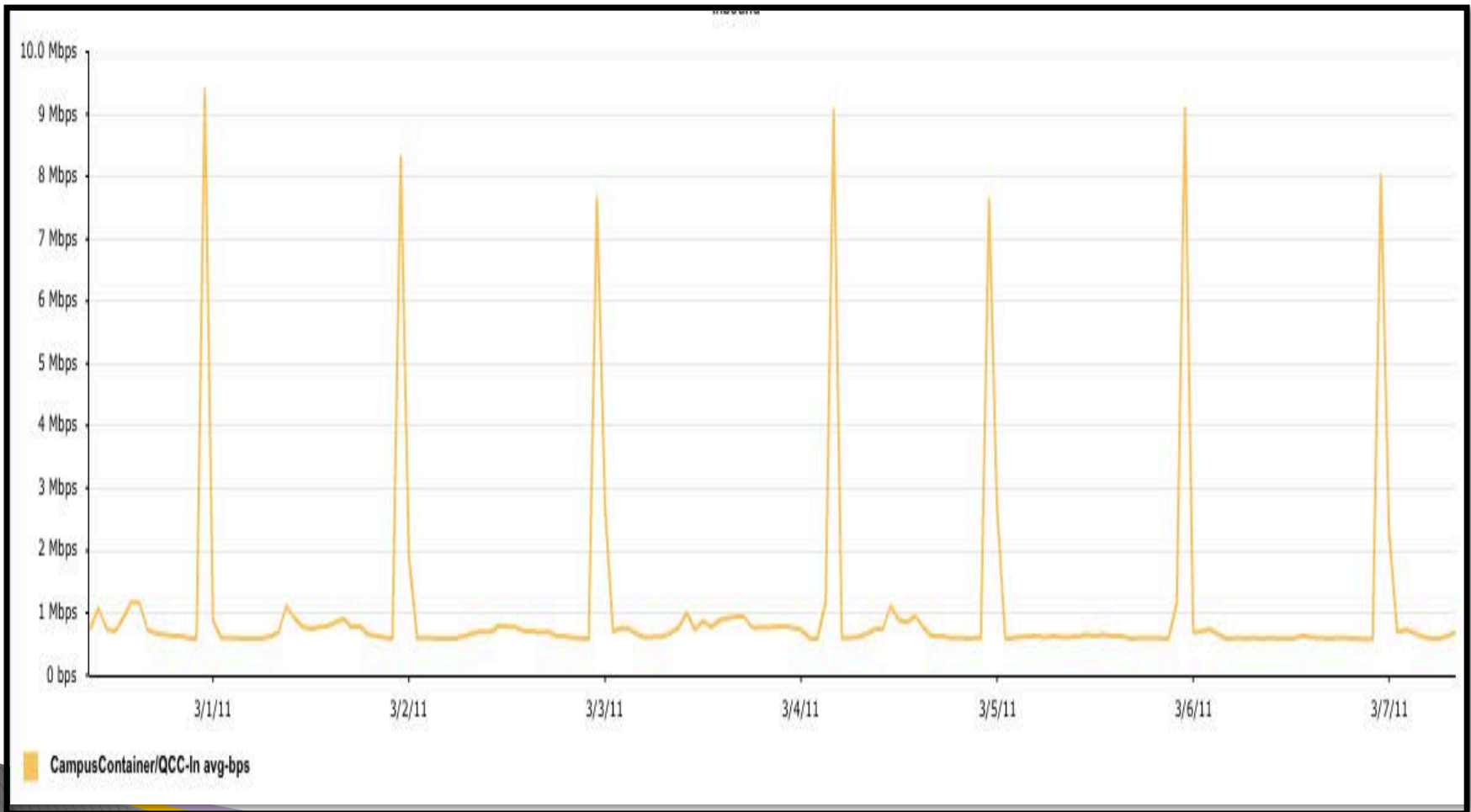


# VPN – Site to Site

- ▶ 3 VPN's from Macomb campus to QC 60<sup>th</sup> St, QC Caxton and QC WQPT
- ▶ 2 VPN's from QC 60<sup>th</sup> St to QC Caxton and QC WQPT
- ▶ Central Management Services (CMS) to Springfield, IL
- ▶ Disaster recovery
- ▶ Portal Tunnel
- ▶ Beu to CTI

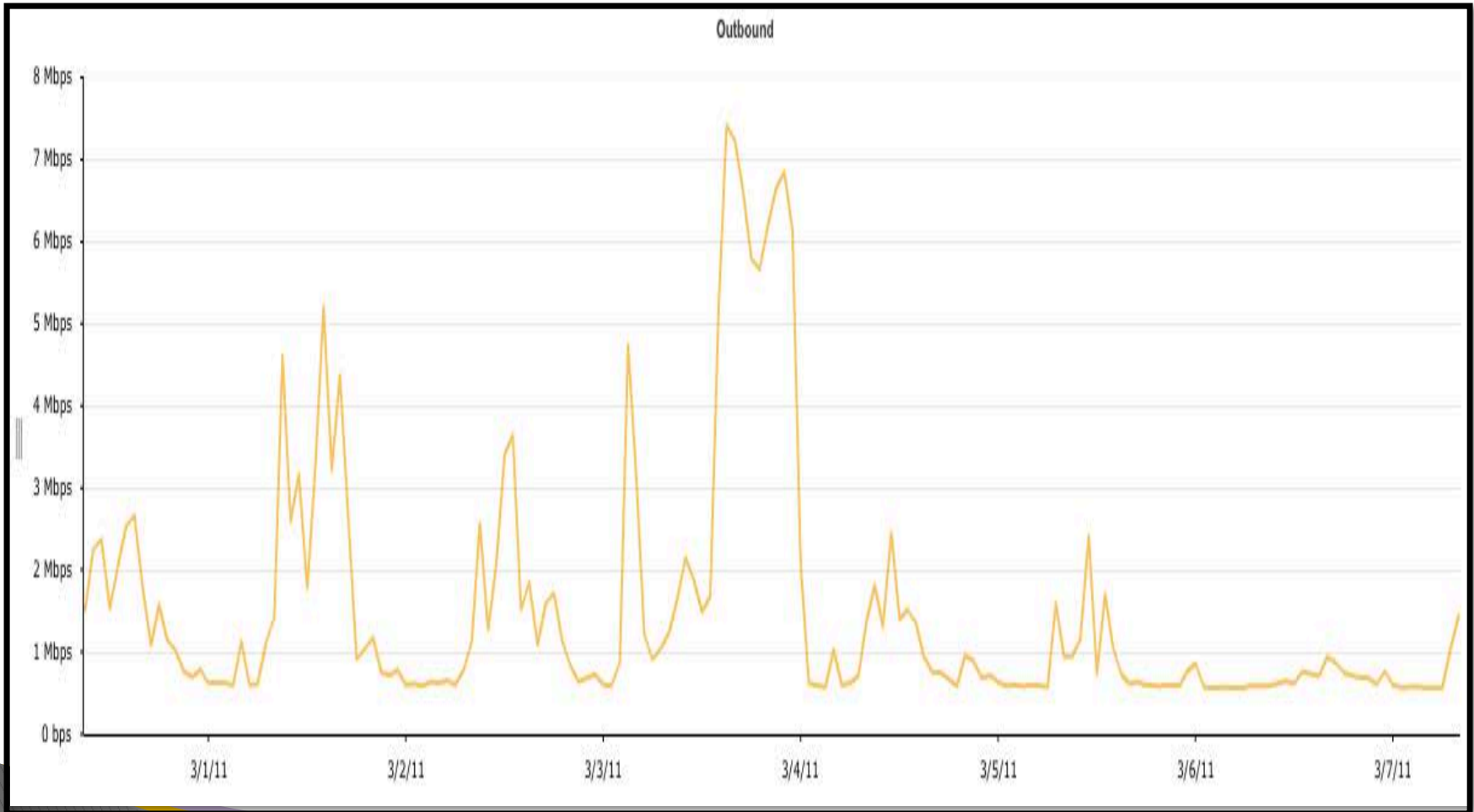


# Macomb to QCC VPN Traffic -Inbound





# Macomb to QCC VPN Traffic –Outbound



# VPN – Vendors

- ▶ Macomb campus – 21 vendor VPN's
  - Laserfiche access for Business Services
  - DVSPORT access for Athletics
  - Nuclear Motion access for Physics
  - LockSmith access for Physical Plant
  - H2IT access to VoIP systems
  - Right Answers access to Western Knowledge Base
- ▶ QC 60<sup>th</sup> St – 1 vendor VPN
- ▶ QC WQPT – 1 vendor VPN



# VPN – Client

- ▶ Cisco AnyConnect Client
  - Does support 64bit OS's
  - Uses SSL for encryption
  - Is set up from a web page <https://vpn.wiu.edu>
  - Is the replacement for the Cisco VPN Client
- ▶ Cisco VPN Client
  - Does not support 64bit Windows system
  - Uses IPsec for encryption
  - Is obsolete (will be discontinued this summer)
  - Currently users of this client are sent an email to ask them to start using the AnyConnect Client

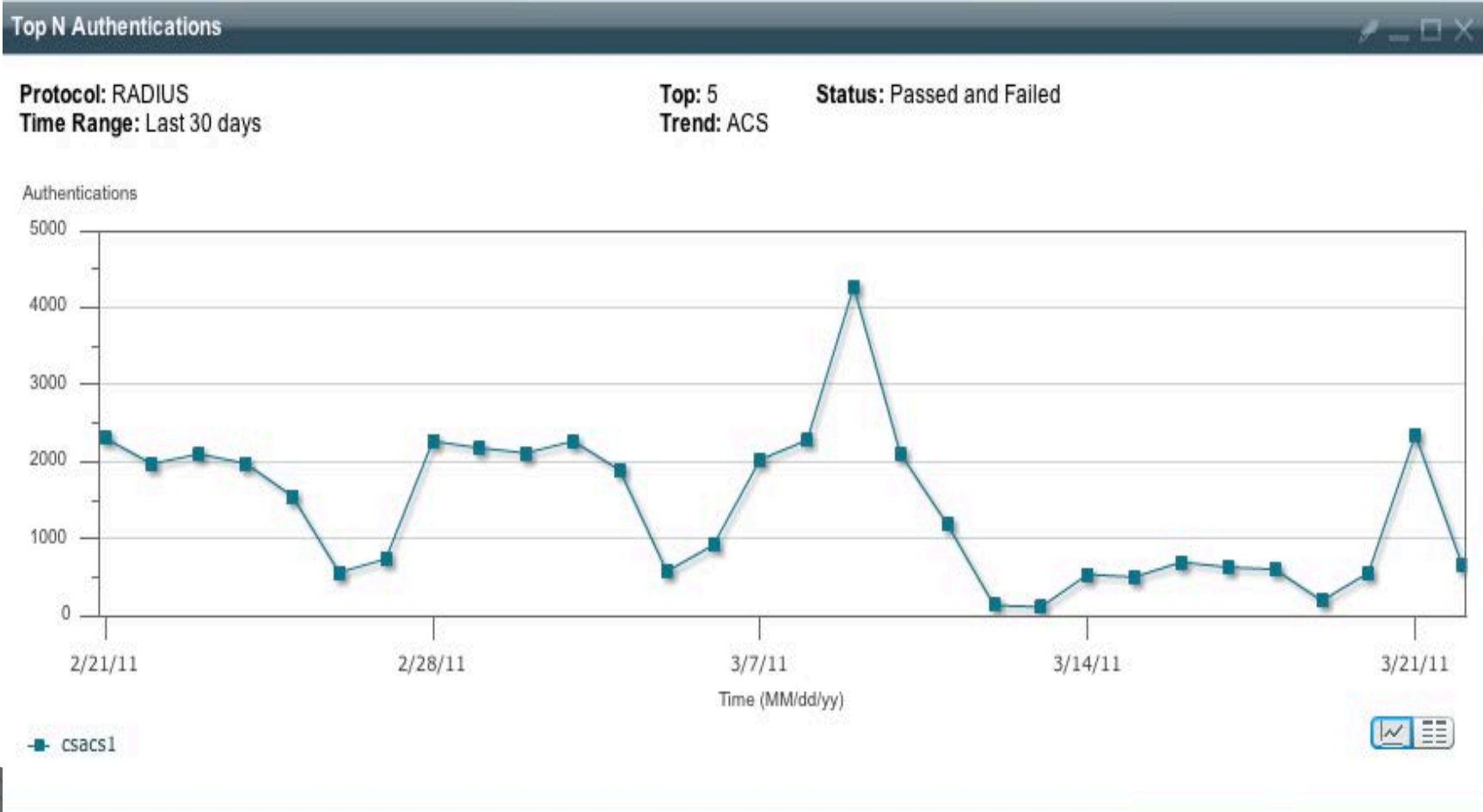
# Authentication, Authorization, Accounting (AAA)

- ▶ **Authentication**
  - Who is allowed access
- ▶ **Authorization**
  - What they are allowed access to
- ▶ **Accounting**
  - What did they access

# Cisco ACS

- ▶ VPN
  - 18 passed authentication per day
- ▶ Secure Wireless
  - 2052 passed authentication per day
  - 125 unique users per day
- ▶ Currently researching how to better manage Authorization and Accounting

# Cisco ACS



# Antivirus

## ▶ SEP11

- New console was brought online by User Support.
- Monitor console.



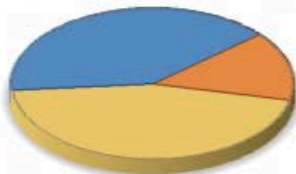
# SEP11 Console

Summary type: AntiVirus and TruScan Proactive Threat

(data for the past 12 hours)

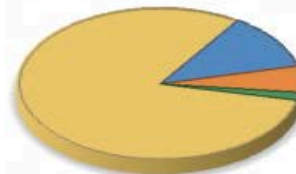
Last updated at: 03/22/2011 14:38:17

## TruScan Proactive Threat Scan



CSGold	9
(Unknown)	8
LogMeIn	3

## Risk Distribution by Source



Scheduled scan	54
TruScan Proactive Threat Scan	8
Manual Scan	4
Auto-Protect scan	1

## Risk Distribution



(Unknown)	5
W32.Spyrat	5
Tracking Cookies	4
Trojan.Maljava	3
Backdoor.Tidserv	2
Other	16

## Risk Distribution by Attacker



No Information	0
----------------	---

## New Risks

Risk Name	Detected By	Computer
Trojan.FakeAV!gen42	Scheduled scan	WMU500462
Trojan.Adclicker	Scheduled scan	WMU510443
Joker	Scheduled scan	WMU507878

3 total risk detections

## Risk Distribution by Group



My Company\ESS Machines	28
My Company\WMU - Macomb	19
My Company\WMU - QC	11
My Company\Laptops	5
My Company\WMU - Macomb\Labs	4

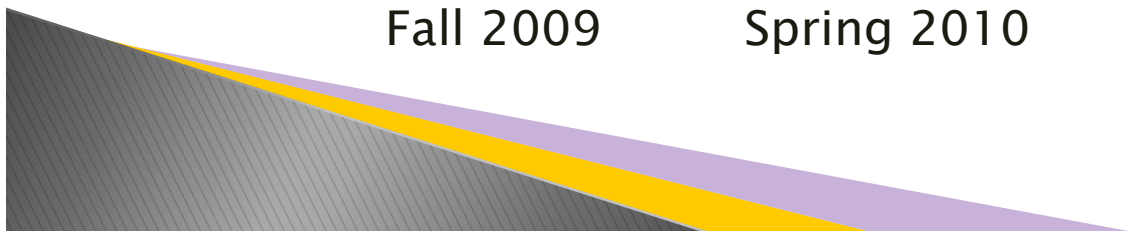
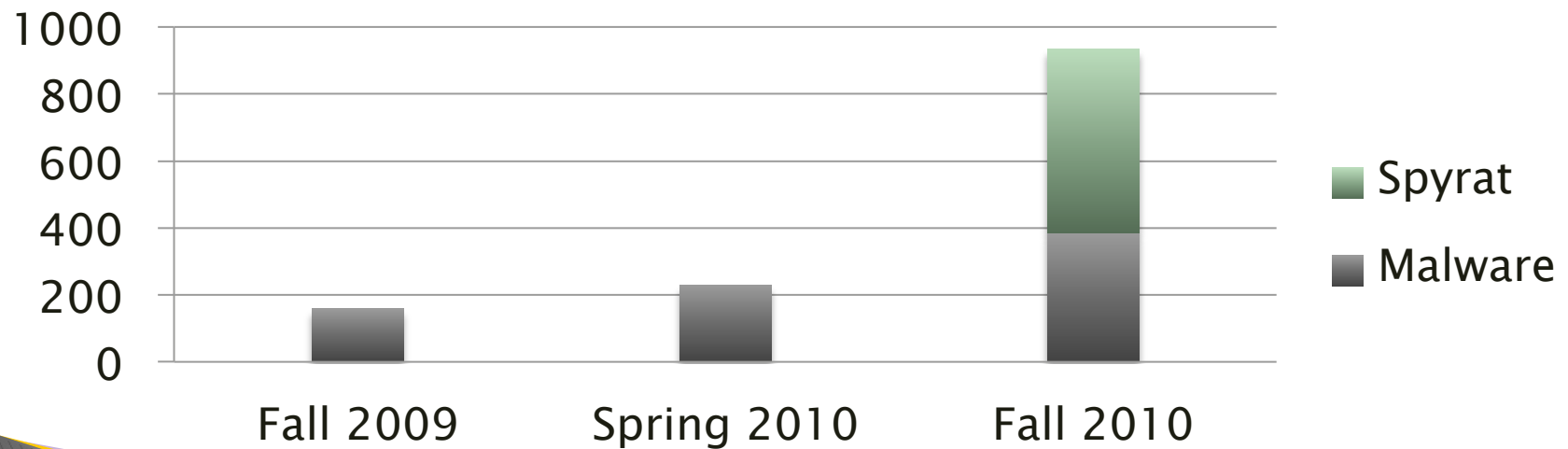


# Malware Procedure

1. Computer is scanned for sensitive data
2. If Sensitive data is found
  1. Sensitive data is removed from computer
  2. Computer is imaged
3. Malware is removed
4. Computer is returned to user in operating condition
5. Risk assessment is done

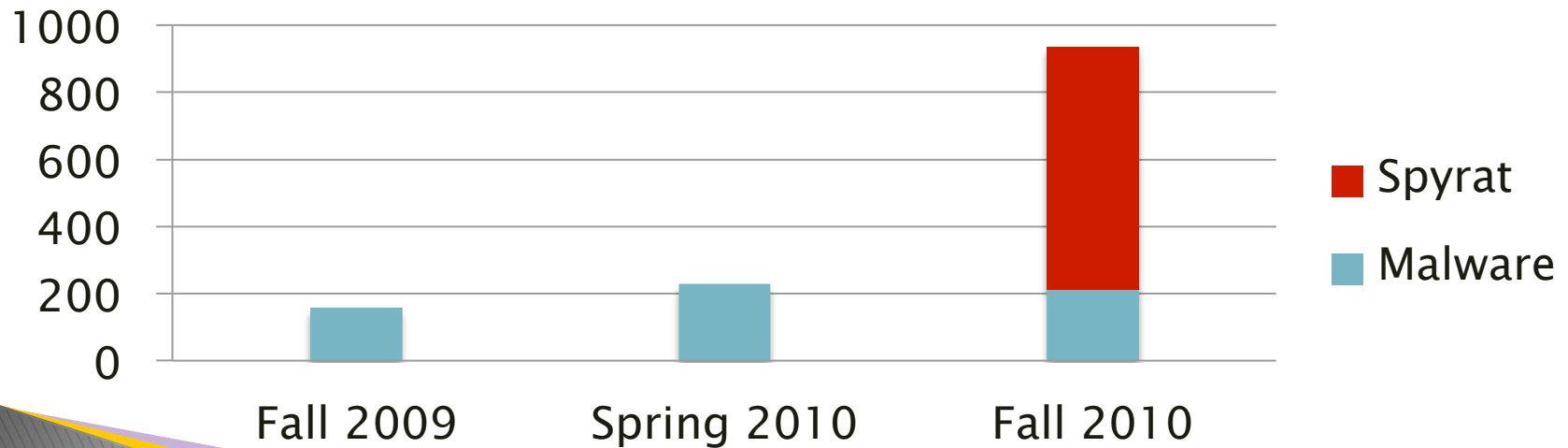
# Malware

	Fall 2009	Spring 2010	Fall 2010
<b>Macomb</b>	150	220	921
<b>QC</b>	9	10	15
<b>Total</b>	159	230	936



# Malware

	Fall 2009	Spring 2010	Fall 2010
<b>Macomb</b>	150	220	921
<b>QC</b>	9	10	15
<b>Total</b>	159	230	936



# Protecting Computers

- ▶ Published monthly Windows patching cycle
- ▶ Symantec upgrade to SEP 11.06
- ▶ Disabled auto-run
- ▶ User Access Control
  - User accounts that are members of the local Administrators group will run most applications as a standard user
  - Most tasks requiring administrative rights will auto-elevate

# SEP11 Console

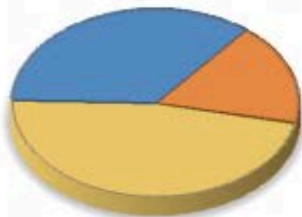
Summary type:

(data for the past 12 hours)

Last updated at: 03/22/2011 14:40:16

## Top Targets Attacked by Group

Display:



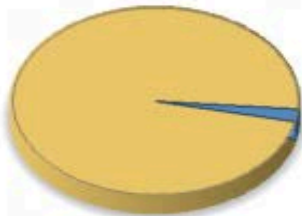
My Company\WLU - Macomb	8
My Company\Laptops	6
My Company\WLU - QC	3

## Top Sources of Attack



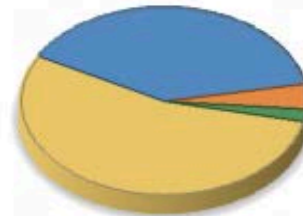
143.43.233.110	96
143.43.235.212	55
143.43.230.15	53
143.43.224.72	19
216.124.189.113	10
Other	43

## Attack Event Types



Intrusion Prevention	270
Port Scan	6

## Security Events by Severity



Info	166
Critical	118
Major	14
Minor	6

# Vulnerability Scans

- ▶ All vulnerability scans are conducted with Nessus
- ▶ Quarterly vulnerability scans are done on all servers
- ▶ Ad-hoc scans are done when a server is requested external firewall changes
- ▶ The 2011 Quarter 1 Vulnerability Report is a 39 page document



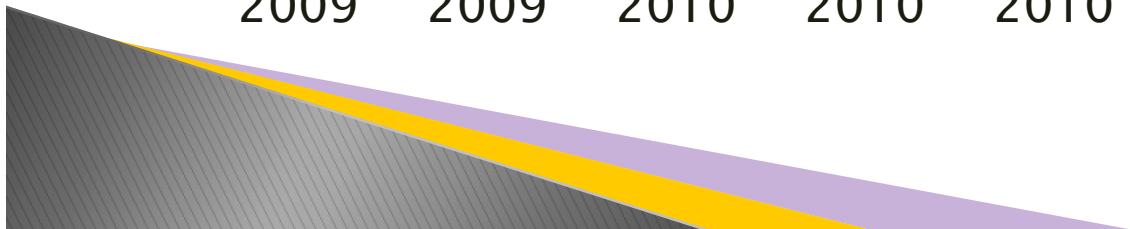
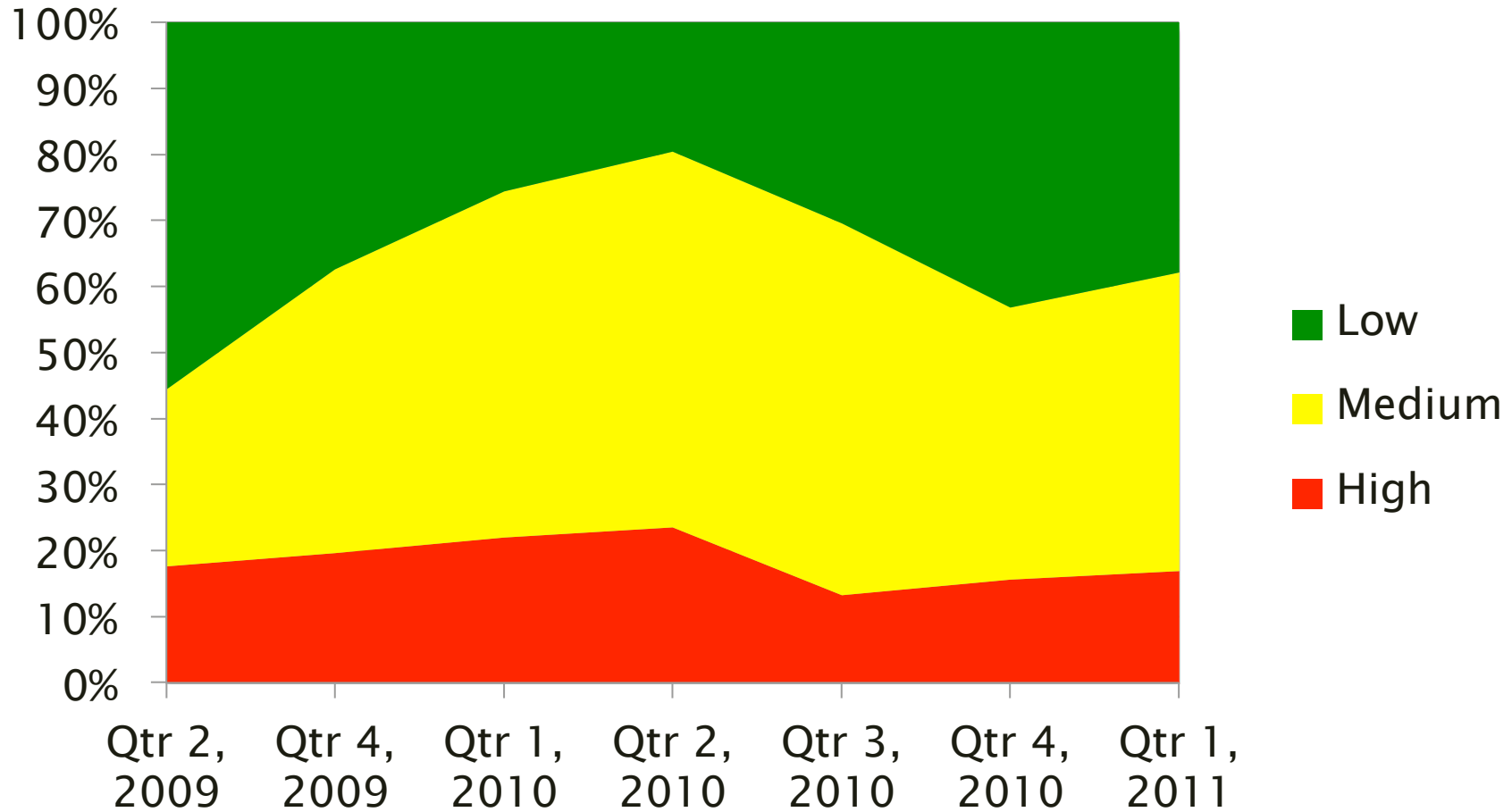
# Qtr. 1, 2011 Results

	Device Count	% of Devices	Total Vuln.
High Level Vulnerabilities	69	17%	136
Medium Level Vulnerabilities	185	45%	1,415
Low Level Vulnerabilities	155	37%	10,255



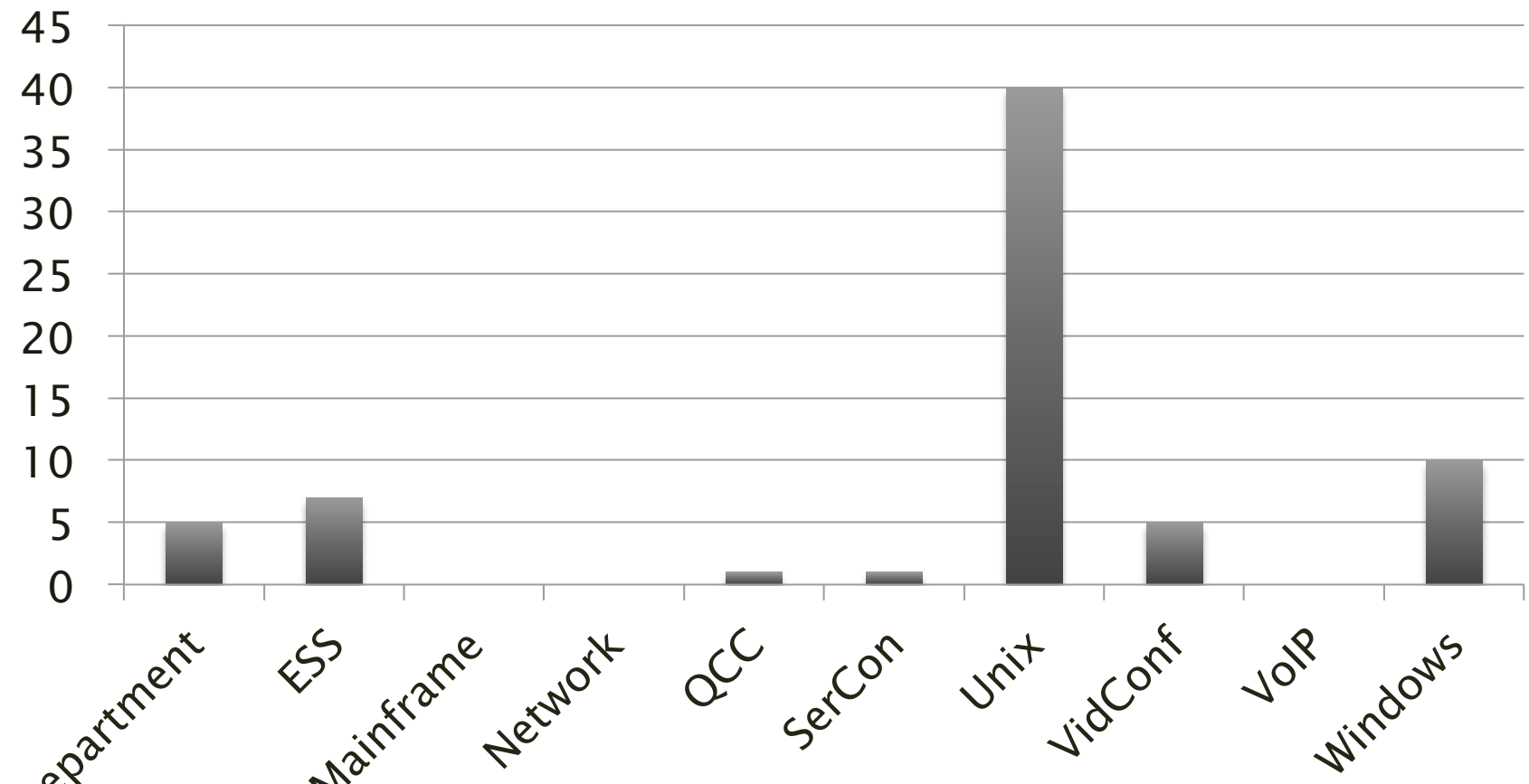
- High
- Medium
- Low

# Vulnerability Scan History

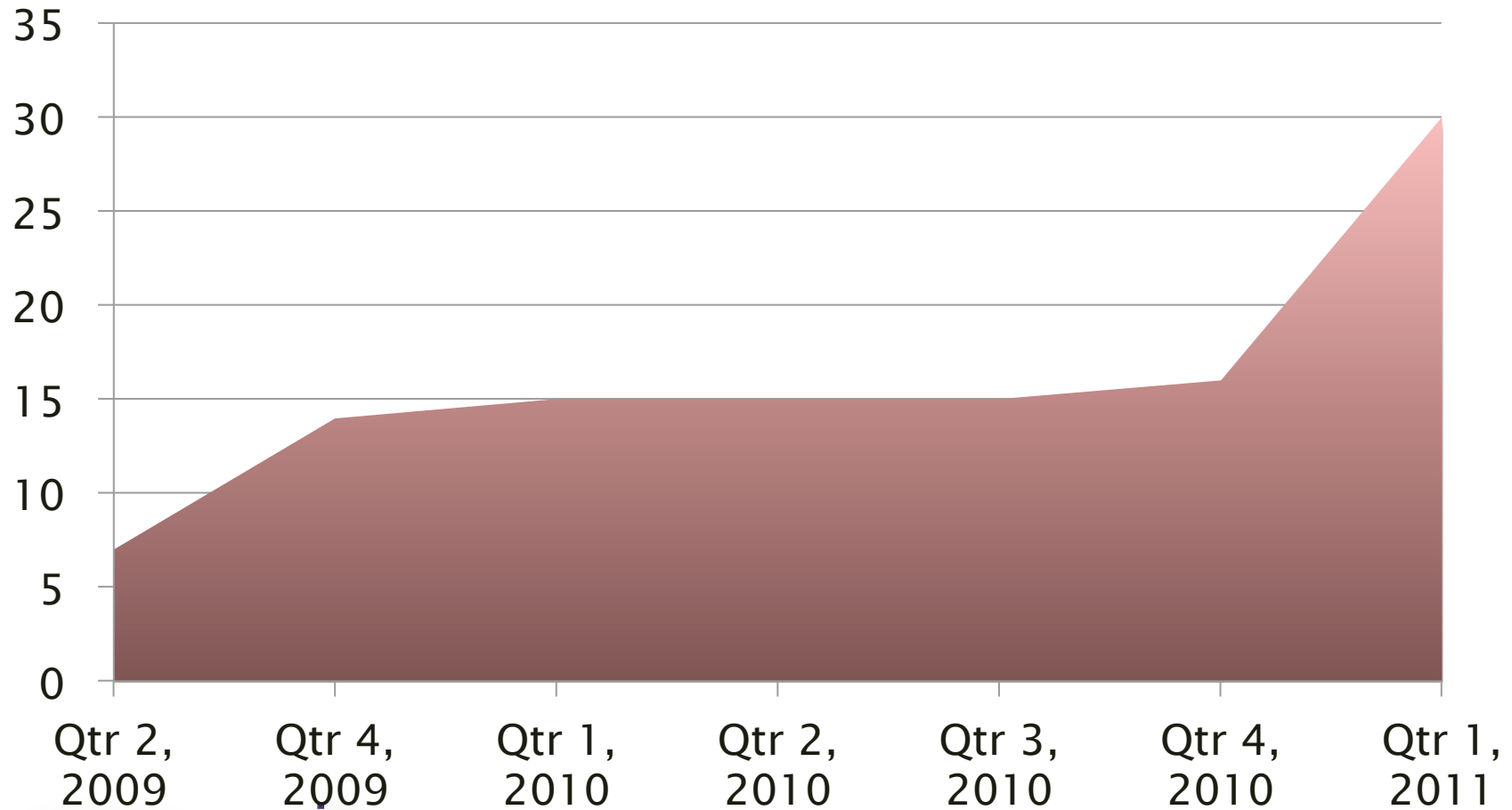




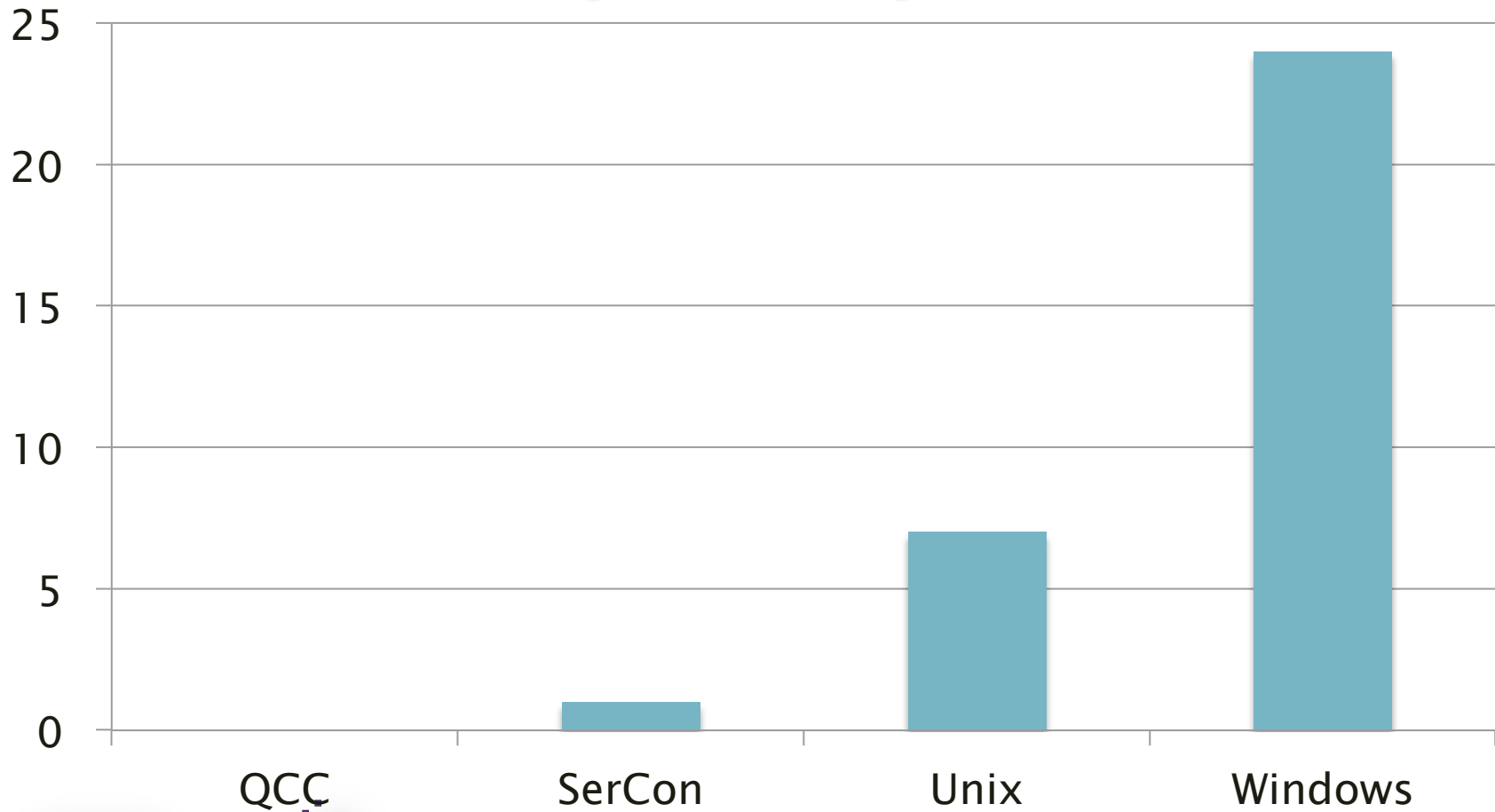
# High Vulnerability by Group



# Qtr. 1, 2011 Lockdown



# Lockdown by Group



# Copyright Notice Procedure

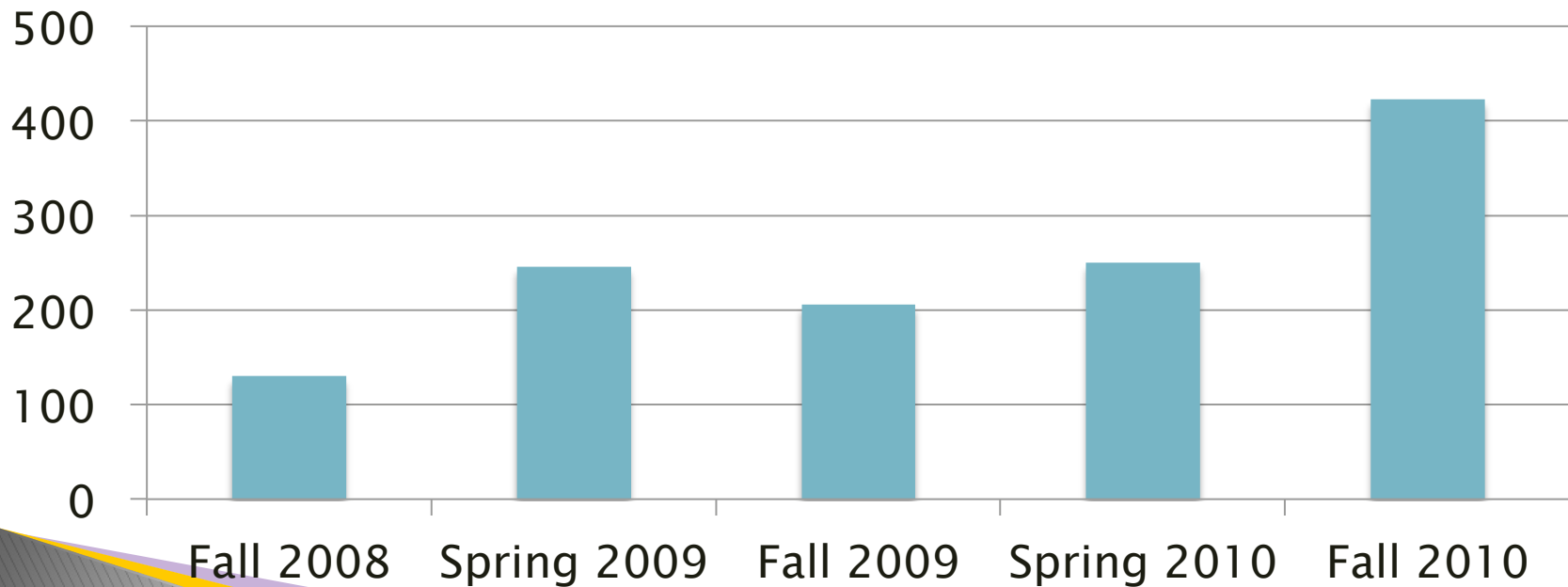
- ▶ ResNet
  - Trace IP in the notice to the room occupants
  - The notice is then forwarded on to the occupants of the room
- ▶ Wireless
  - Since we cannot trace on our wireless network, all wireless notices are discarded
- ▶ Campus
  - Trace IP in the notice to the computer
  - Notify the user and their supervisor of the infringement

# Copyright Notices Received From

- ▶ BayTSP
- ▶ Business Software Alliance (BSA)
- ▶ CBS Corporation
- ▶ Columbia Pictures Industries Inc.
- ▶ Home Box Office, Inc. (HBO)
- ▶ Lionsgate Films
- ▶ Lucas Arts
- ▶ Media Factory
- ▶ Media Sentry
- ▶ NBC Universal
- ▶ Paramount Pictures Corporation
- ▶ Recording Industry Association of America (RIAA)
- ▶ Sony Pictures Entertainment
- ▶ Universal Studios
- ▶ Video Protection Alliance Services (VPA)
- ▶ Warner Bros. Entertainment Inc.
- ▶ Worldwide Sony Pictures Entertainment Acquisitions Inc.
- ▶ Zuffa LLC

# Notices to Date

	Fall 2008	Spring 2009	Fall 2009	Spring 2010	Fall 2010	Total
<b>Macomb</b>	130	246	206	250	423	963
<b>QC</b>	0	0	0	0	0	0



# Identity Protection Act (Public Act 096-0874) Efforts

- A Credit Card handling policy and an updated SSN policy approved by the President's cabinet in August 2010
- Annual Credit Card handling training in place since 2008
- Regular sensitive data handling training in place since January 2011



# Sensitive Data Scans

- ▶ Sensitive data scans started Fall 2009
- ▶ Seek-N-Secure (SNS) is the application used for scans
  - Automatically installed on all Windows computers using AD
  - Manually installed on all Macintosh computers
  - Currently being installed and tested on servers

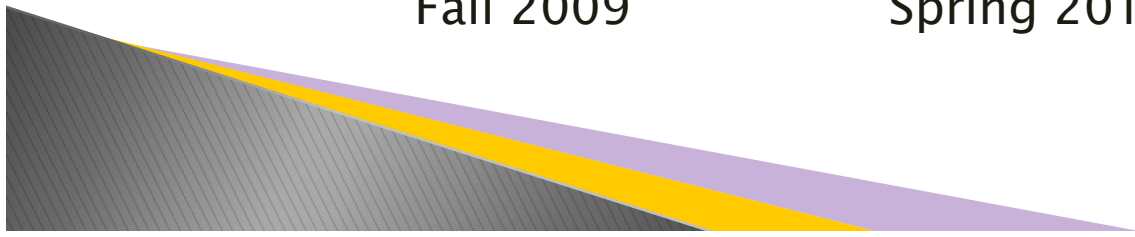
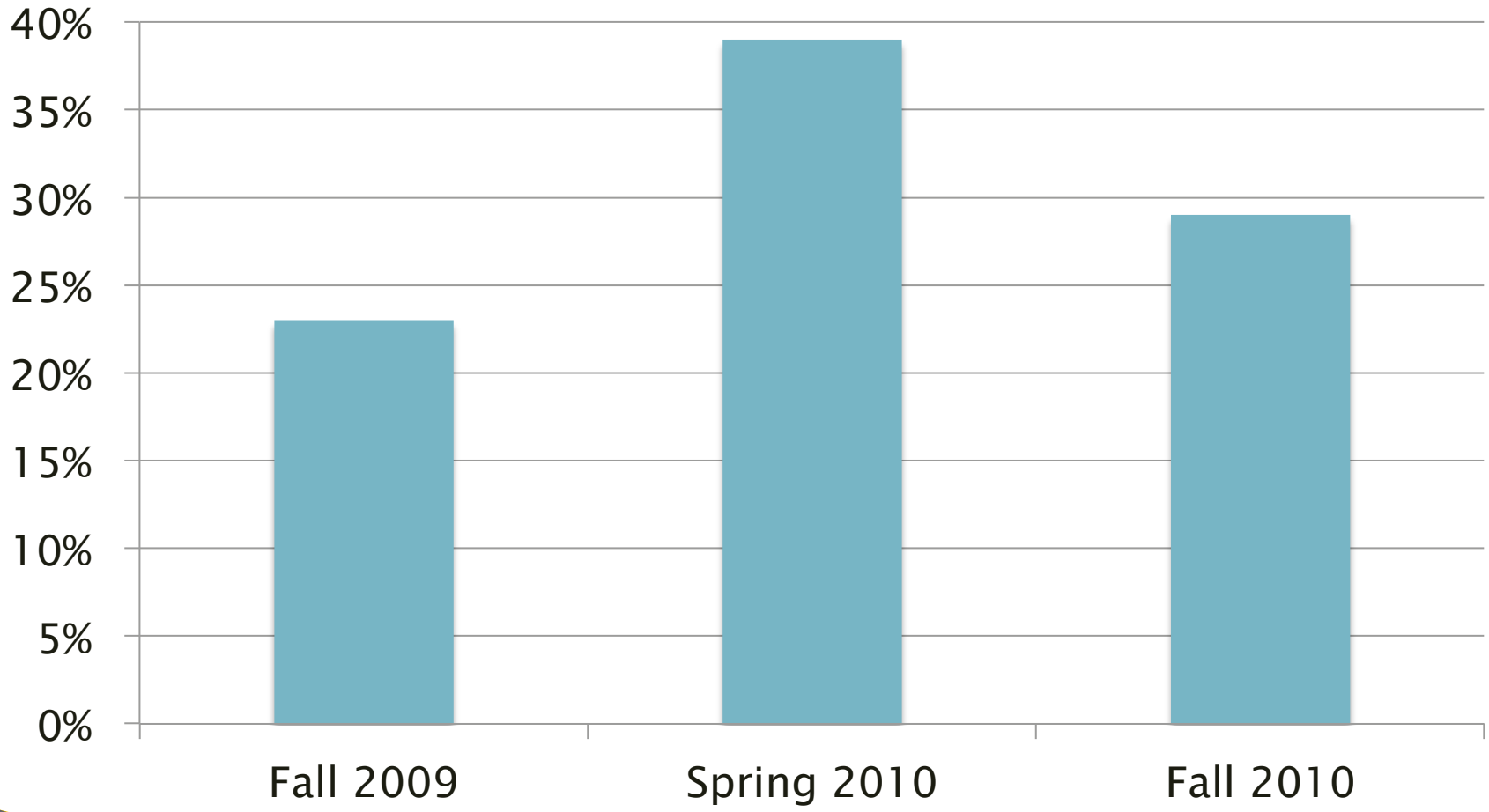




# Sensitive Data Scans Procedure

- ▶ All Windows computers are scanned semi-annually, except labs
  - This is limited to Windows based computers for now
- ▶ All computers with Malware are scanned
- ▶ All computers with data transfers are scanned before data is transferred
- ▶ Server scans are starting in the summer of 2011

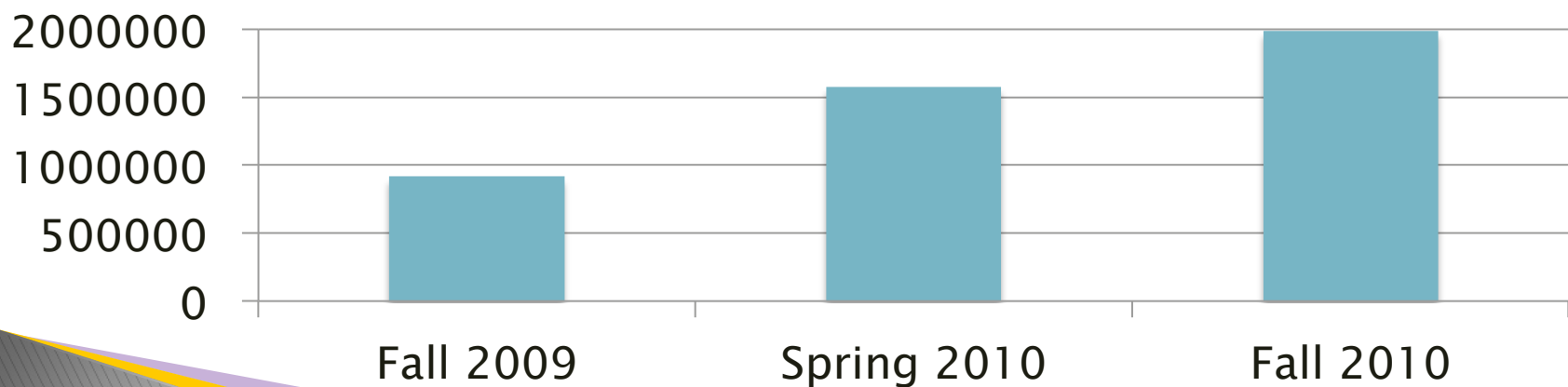
# % Computers with Data on Semi-Annual Scans



# Semi-Annual Scan Results

Semester	Files Scanned.	CC	SSN
Fall 2009	2,192,062	6,951	909,113
Spring 2010	144,440,332	43,403	1,534,979
Fall 2010	117,190,775	13,997	1,977,313
Total	283,557,149	64,351	4,421,405

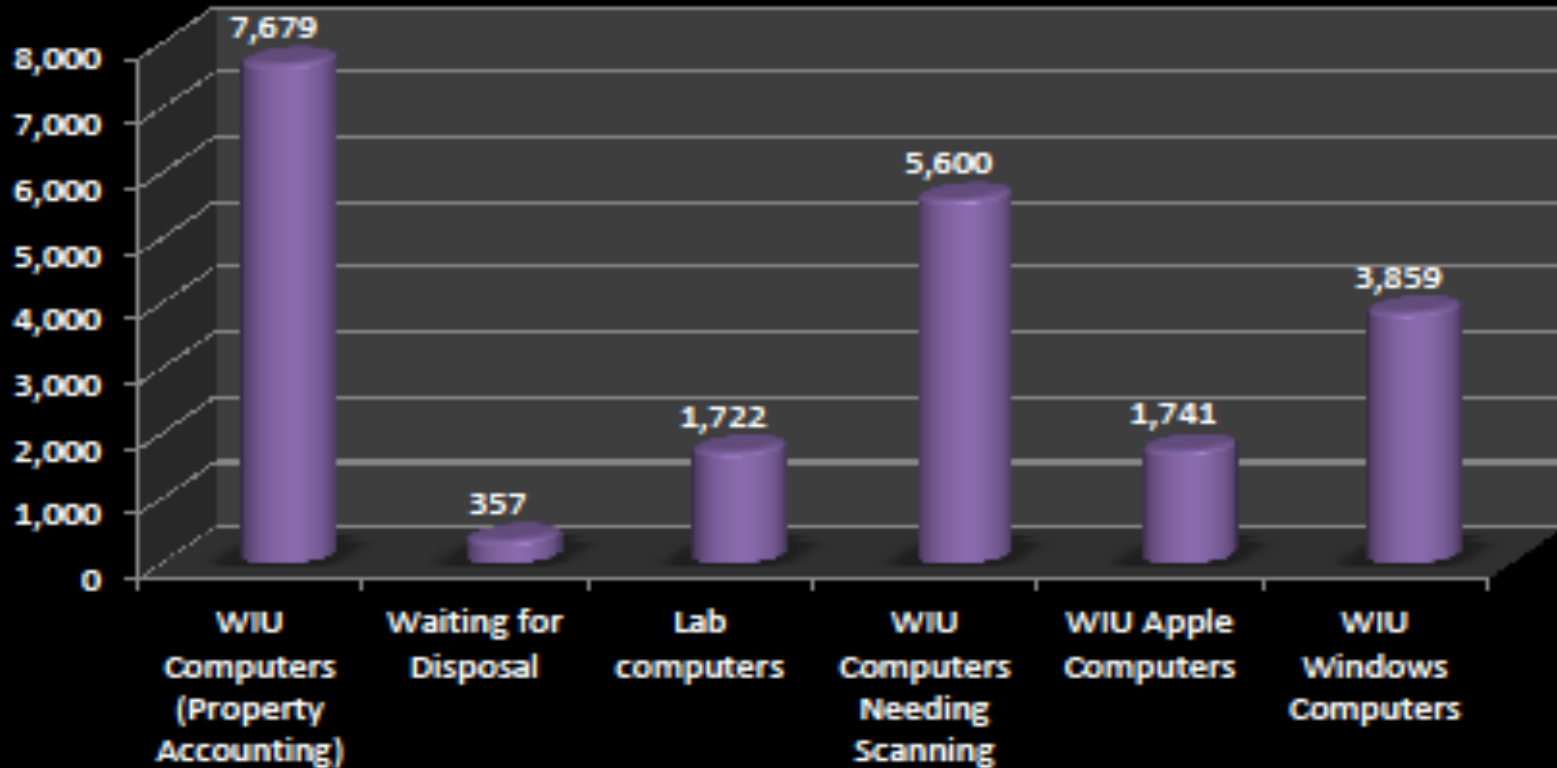
## Total Sensitive Data Found



# In Scope WIU Computers

(currently only Windows)

## WIU Computers Needing SnS Scanning



# Where Have All The WIU Computers Gone?

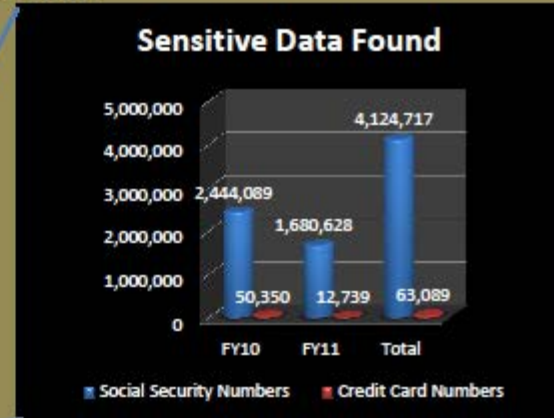
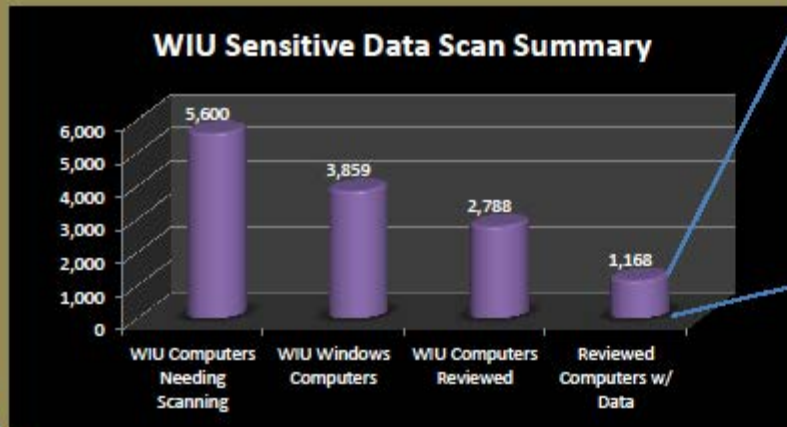
(Based on Property Accounting Data)

- ▶ Purchase of Approximately 4,050 Computers Preceded the University SSN Policy
  - 2007 Through 3/28/07 – 106 computers (Original SSN Policy Approved 3/30/07)
  - 2006 – 1,009 computers (4 years old or older)
  - 2000–2005 – 2,806 computers
  - 1990s – 124 computers
  - 1980s – 5 computers (including 1 from 1985)



# WIU Sensitive Data Scan Summary

August 2009 - October 2010



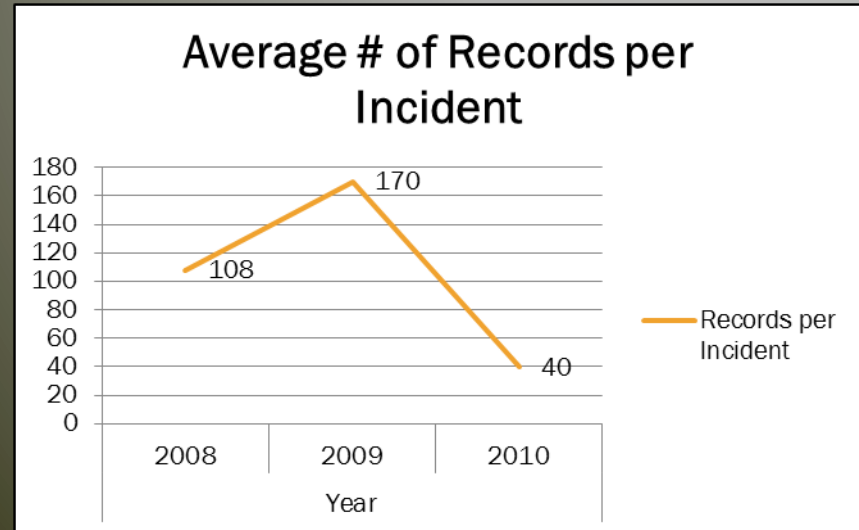
Office of the CTSO

October 2010

- ▶ With 72% of Windows computers scanned
  - ▶ 42% of computers contain sensitive data
  - ▶ 3 cents per record cleaned vs. \$204 on average per record to notify

“The truth will set you free. But first, it will piss you off” – Gloria Steinem

Year	Number of	
	Incidents	Records
2006	1	180,000
2008	1	108
2009	4	681
2010	4	158



- ▶ 10 incidents since July 2006 have required WIU to notify nearly 181,000 individuals and the Illinois General Assembly of possible data leaks
- ▶ Additionally Western experienced 2 FERPA data leaks in 2010

- ▶ With support from ESS cleaned 279 computers in the Division of Student Services in 6 weeks
  - Vice President Student Services
  - Financial Aid
  - Brooks Cultural Center
  - Casa Latina
  - Womens Center
  - Career Services
  - Counseling Center
  - Disability Support Services
  - Veteran Center
  - Student Legal, Student Judicial, Student Development
  - Student Activities, Student Government, Student Organization Center, Student Assistance & Parent Service Center
  - Union Admin offices & Union Service Center





# Disaster Recovery

- ▶ Together with AIMS and Financial Aid successfully tested the recovery of the Financial Aid Interface System from the SunGard facility in Chicago
- ▶ Off Site Storage for uTech (Systems, Enterprise Systems, Telecom) and ESS Moved to QC

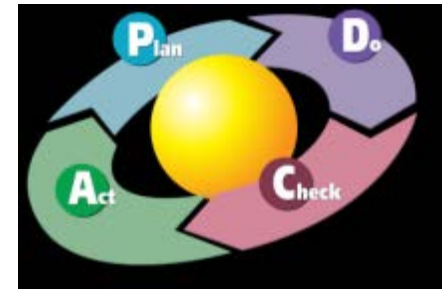


# Technology Security

»» FY12 Priorities

# Identity Protection Act Efforts

- ▶ Plan – Survey SSN Usage and Hire DBA (or make extensive use of consultants)
- ▶ Do
  - Risk Assessments
    - VP Approved Justification for Sensitive Data
    - VP Approved Plans to Protect Data in Transit and at Rest
  - FTP, Email, Databases, Mainframe
- ▶ Check – Audit
- ▶ Act – Improve



“If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.” — Bruce Schneier

# Identity Protection Act (Public Act 096–0874) Efforts – Cont

- SnS Scanning for SSN and Credit Card Data
  - Ongoing scanning – March/April and October/Nov
  - Extend scanning to Macs including Macs running Windows using Bootcamp or within a virtual environment
  - Extend Scanning to Windows, Mac, Solaris, and Linux Servers
  - Extend Scanning to Email Archives
  - Extend Divisional scanning beyond the Division of Student Services



# Secure Wireless

- × Security Model Proposed Spring 2008
  - + New secure wireless network coexists with current open wireless network
  - + PCI DSS specific secure wireless network created for areas that must take cards over wireless
  - + Open wireless network modified to only allow limited Internet access
- × Next Step – Xpress Connect and communications plan

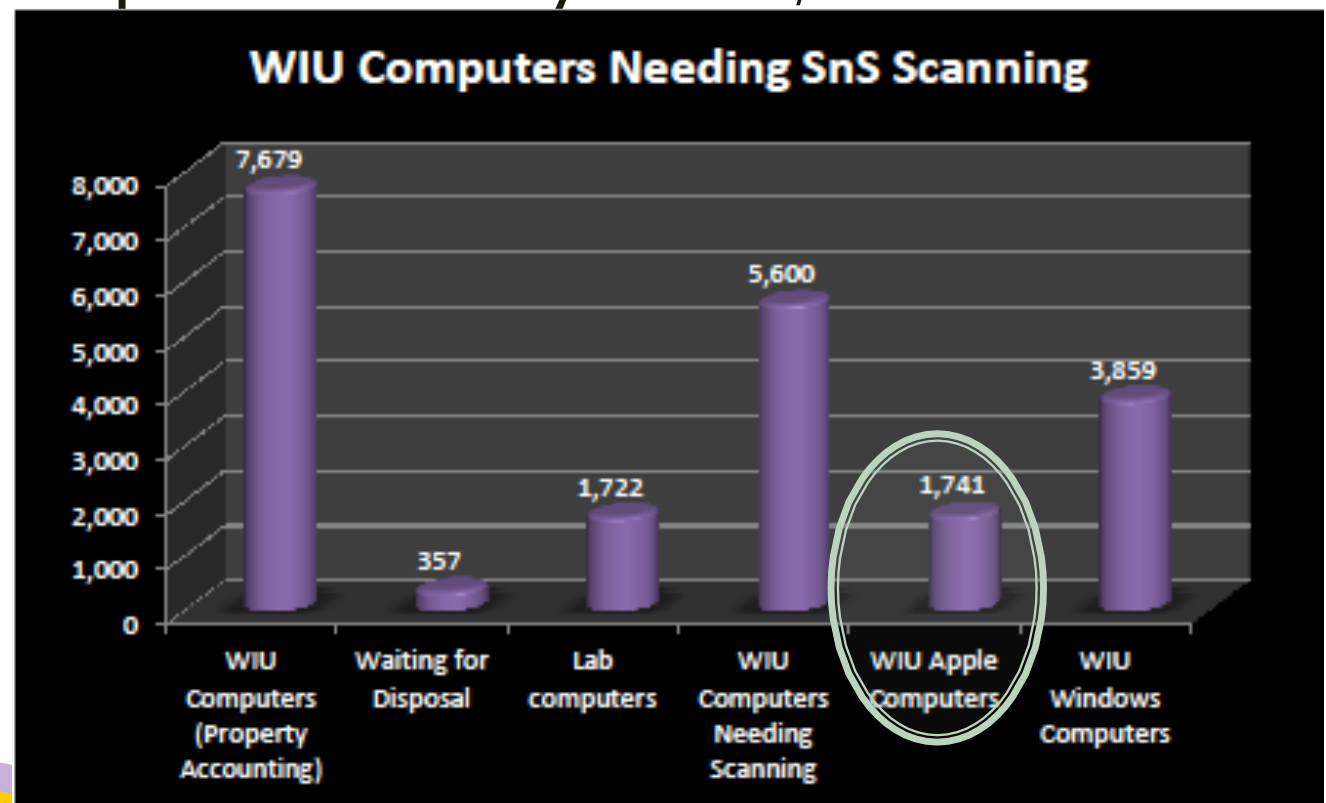


# What Can We Learn From Spyrat?

- ▶ 725 infected university computers including 2 Servers
- ▶ 335 non lab computers SnS scanned
  - 23 computers had 478 CCs and 5,247 SSNs
  - 30% never scanned

# Never Been SnS Scanned

- ▶ Extend Divisional scanning beyond the Division of Student Services
- ▶ The Need for Open Directory LDAP/AD Integration



# What Can We Learn From Spyrat?

- ▶ 725 infected university computers including 2 Servers
- ▶ 335 non lab computers SnS scanned
  - 23 computers had 478 CCs and 5,247 SSNs
  - 30% never scanned
  - 57% had data in temp internet files or Recycle Bin



# Managing Internet Files & Recycle Bins (opt-in to or opt-out of University provided protection)

Western Illinois University University Technology

Admissions | Academics | Student Life | About WIU | Arts | Athletics | Alumni | Home

uTech Menu

Guests  
Faculty  
Western Online  
Computer Tools  
Help Desk  
Email Us

Your session will expire in 457 seconds

## GUIAVA

Graphical Unix Administration Validation Assistant

Server Services Menu

Home Password Web Servers E-Mail Personal Support Center

Level: 1 of 10000

Settings	Status
MySQL	Disabled
SMTP Email Support	Disabled Disable (Default) Enable
Virtual Private Network (VPN)	Disabled Disable (Default) Enable
Delete Temporary Internet Files	Enabled Enable (Default) Disable (Not Recommended)
Empty Recycle Bin	Enabled Enable (Default) Disable (Not Recommended)

following set of tools can install, remove, change administrative passwords and look at the status of MySQL.

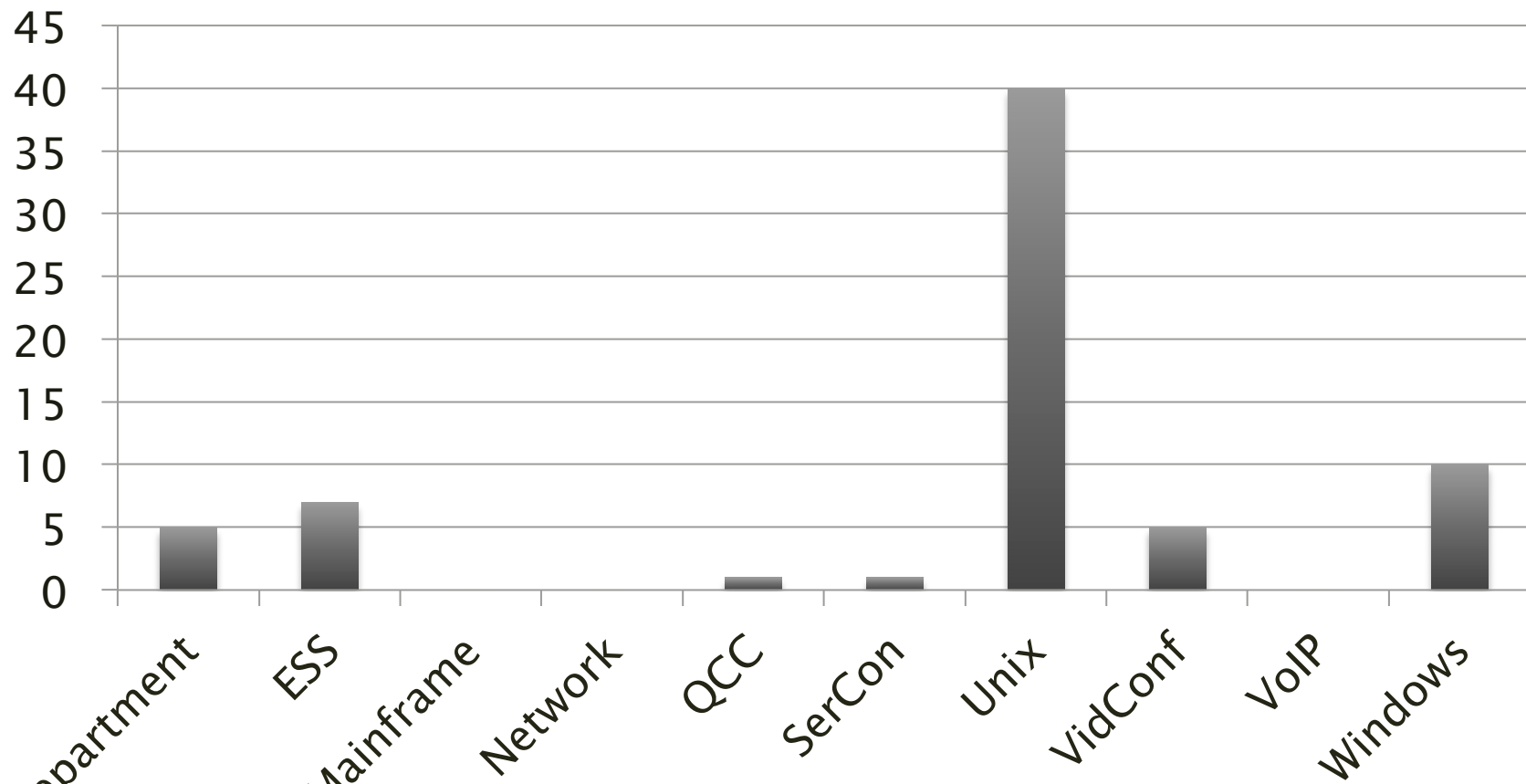
### Western Online Course Tools

These tools are for instructors to activate and migrate courses to Western Online.

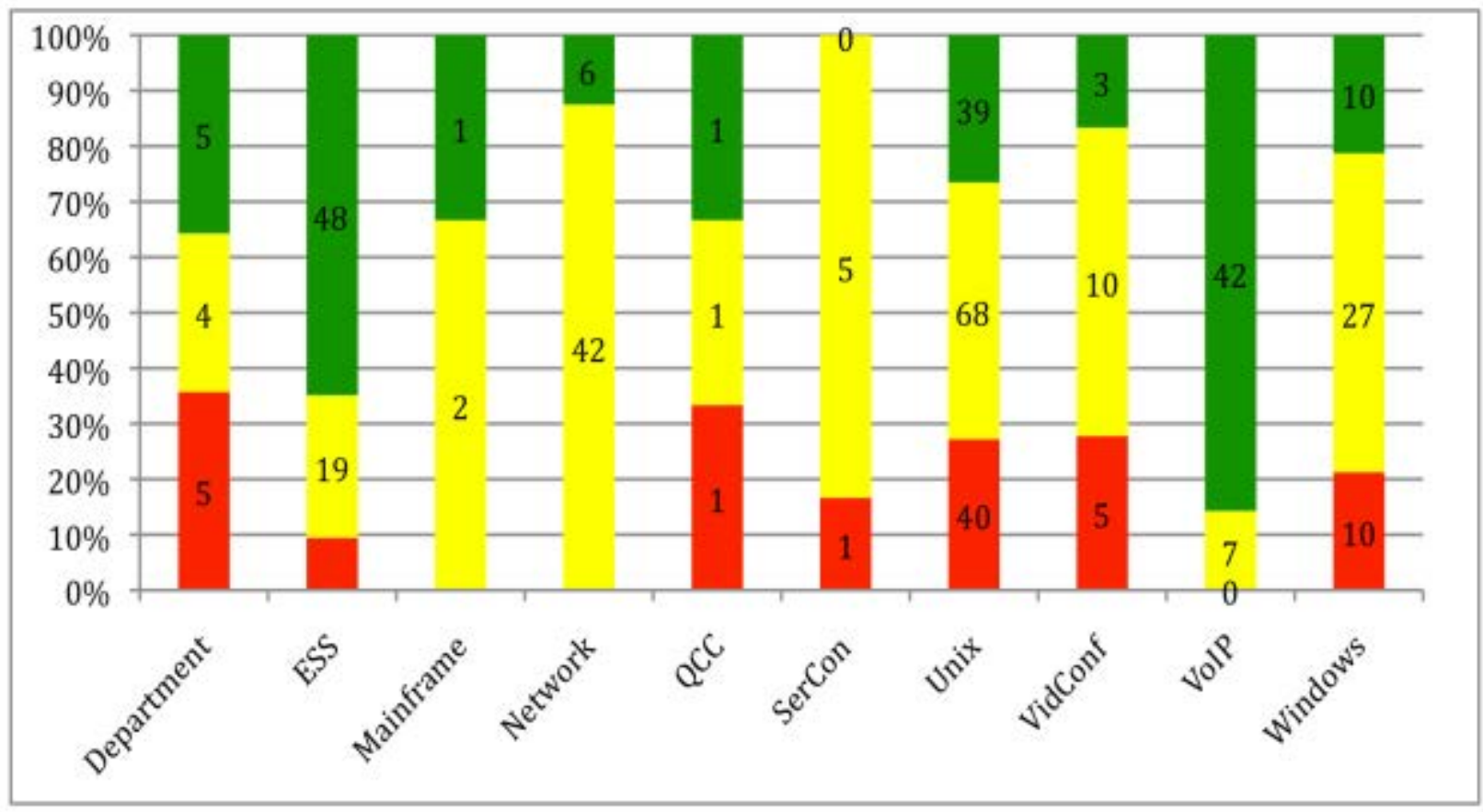
# Symantec SEP Vendor Recommendations

- ▶ Evaluate the Symantec firewall for possible replacement of the built-in OS firewall
- ▶ Move away from using an internal SEP console database

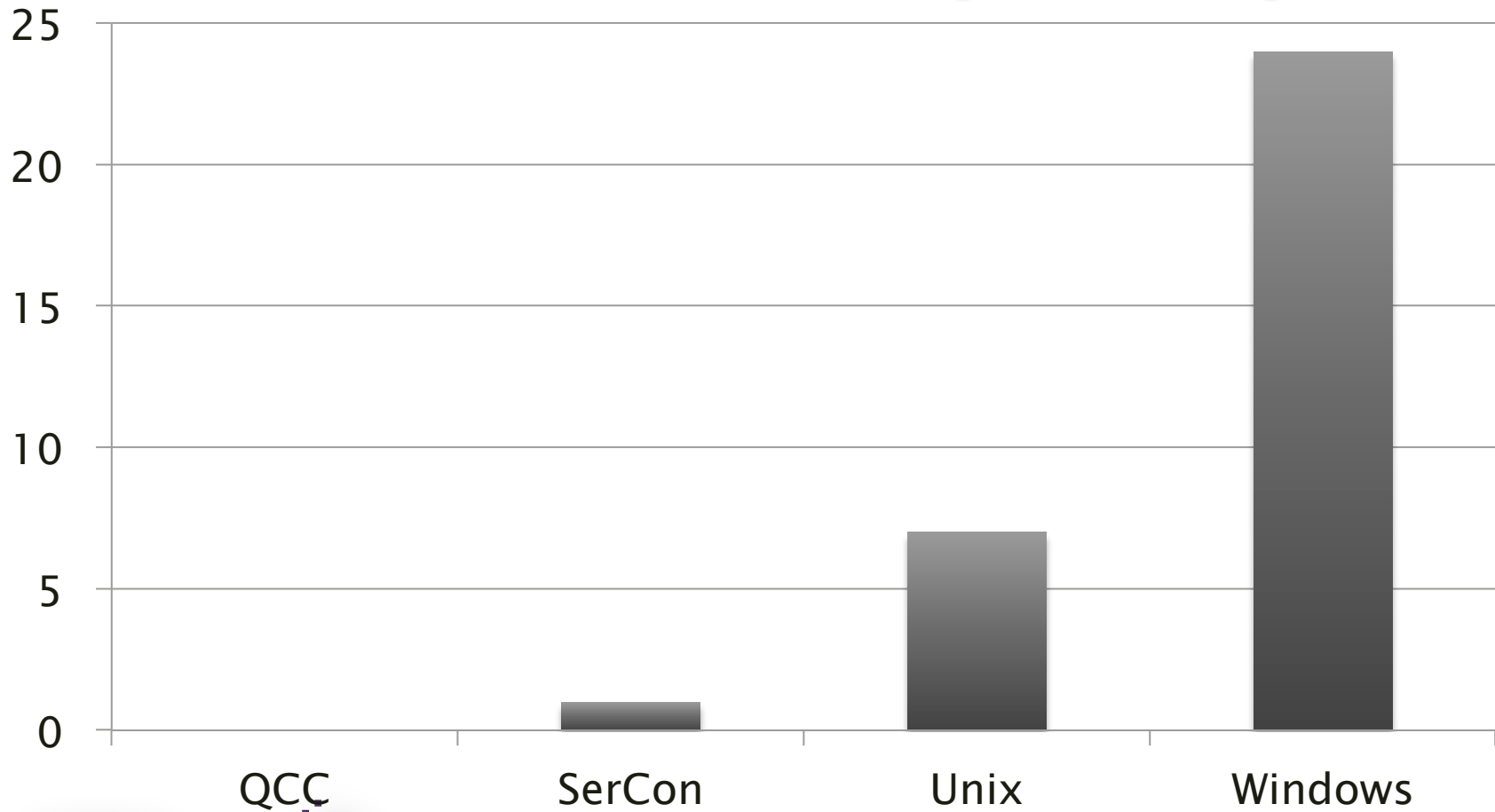
# Server High Vulnerability by Group



# Server Vulnerability Scanning



# Server Lockdowns by Group



# Server Security Project

## (Focus on Risk)

- ▶ Baseline AV/Patching
- ▶ Extend SnS Scanning to Windows, Mac, UNIX, and Linux Servers
- ▶ Resolve Critical/High Vulnerabilities
- ▶ Complete Server Lockdowns
  - Submit forms to admin office
- ▶ Server Business Continuity
- ▶ Administrative Password Policy Compliance



# Disaster Recovery

- ▶ Together with AIMS test recovery of the Automated Payments System from the SunGard facility in Chicago on June 7th.
- ▶ Extend DR/BC testing to Servers, Network, VOIP, and QC





# Payment Card Industry (PCI) Data Security Standards (DSS) Compliance

- × Status of PCI compliance as presented to Presidents Cabinet in 2010
  - × 55+ University Merchants IDs
  - × Over half are considered complex merchants requiring compliance with all 220+ requirements in DSS 2.0
  - × Funding Model – Northern Illinois University and University of Illinois model
  - × Biggest need is the hire the services of a PCI approved Qualified Security Assessor
- × Update: Bank of America & Citizens bank have asked for proof of compliance. Global Payments has implied that they will do the same



# Use of QSAs in Illinois Higher Education

- ▶ Trustwave
  - Northern Illinois University
  - University of Illinois
  - Illinois State University
- ▶ Coal Fire
  - State of Illinois Treasurer's Office



# Hire DBA (or make extensive use of consultants)

- ▶ Illinois universities such as University of Illinois, SIUC, Illinois State and EIU average 4 Information Security FTEs. At WIU Technology Security covers security, policy, awareness, compliance, DR, privacy and DMCA warnings with a CTSO and about 70% of a Technology Security Specialist.



# Questions?

