Why endpoint security?

End user devices are among the most vulnerable parts of an IT infrastructure. To help mitigate the vulnerabilities associated with these devices, the University of North Carolina at Charlotte has focused on leveraging built-in tools that secure these endpoints and reduce costs by leveraging tools that already exist.
ANTI-VIRUS

Endpoint Computer Activity Status

- 1083 Active
- 197 Inactive 2+ Weeks
- 99 Inactive 2+ Months
- 12 Not Protected

Endpoint Protection Client Status

- Total active clients in this collection protected with Endpoint Protection: 95.7%
- Total devices in this collection: 6625
- Endpoint Protection clients in this collection that are active: 5154
  - Active clients protected with Endpoint Protection: 5890
  - Active clients at risk: 264
- Clients in this collection that are inactive or not installed: 471
  - Endpoint Protection agent not yet installed: 21
  - Endpoint Protection agent not supported on platform: 0
  - Configuration Manager client inactive: 408
  - Configuration Manager client not installed: 42
MALWARE AND BOTNETS
NEW ACTIVE DIRECTORY SCHEME
ENCRIPTION
Bitlocker and FileVault
Central Key Store
New Standard
VULNERABILITY SCANS
MONTHLY PATCHING

Missing Updates by Category

- Security Updates: 345
- Critical Updates: 442
- Others: 947
- Updates: 11

ITS, 20%, 80%
OPERATING SYSTEM UPGRADES

OS X El Capitan
PCI

CID
(American Express)

CAV2/CID/CVC2/CVV2
(all other payment card brands)

Chip
PAN
Cardholder Name

Expiration Date

Magnetic Stripe
(data on tracks 1 & 2)
THIRD-PARTY PATCHING
OFF NETWORK MANAGEMENT
PRINTERS
Open Relay
Separate VLAN
Security Checklist
IDENTITY FINDER
DUO

Password + Proof = Access

Password: 

Proof: Is that you?

Access: Success!
PHISHING SIMULATIONS

“95% of all attacks on enterprise networks are the result of successful spear phishing”

Source: Allan Paller, Director of Research - SANS Institute
LESSONS LEARNED

• Have the people who "care the most" "own" the service
• Everything takes time and thoughtful planning
• Use planned/phased rolls outs when able
• Have policy align with practice e.g. encrypting the mobile devices