How to Kill Worms and Viruses with Policy Pontifications

Scott Bradner
University Technology Security Officer
Harvard University
sob@harvard.edu
new title (for me)
continuing (Harvard) responsibilities
but now formalized
“University Technology Security Officer”
“technology” because no management of police
tasks
helps coordinates ways to ensure compliance to laws
  watches out for new laws
coordinates development, implementation &
  administration of high-level security policies
helps coordinate security awareness programs
advises CIO
facilitates security & privacy aware culture
monitors security risks
does he actually do anything himself?
Can he?
Harvard looks Like
Reality

FAS

GSD

LAW

SPH

RAD

HMS

HBS

DIV

GSE

JFK

worm policy 6
actually, real reality is worse in technology

research lab

research lab

research lab

research lab

research lab

research lab

research lab

research lab

research lab

research lab

research lab

research lab

research lab

research lab

research lab

research lab

research lab

research lab

research lab

research lab

research lab

research lab

research lab

research lab

research lab

research lab

research lab
times are changing
but are not yet changed

“ETOB” no longer
a legit reason
so what can he do?

since assertions of central control falls on deaf ears

chair University Technology Architecture Group (UTAG)

“CIOs” from around the University

vets new technology ideas

e.g. PIN system, LDAP directory

discussion of policies

e.g. wireless nets

work with RMAS & OGC

be a visitor
laws can be used as a stick
FIRPA (Family Educational Rights and Privacy Act) privacy of educational records and directory information
HIPPA (Health Insurance Portability and Accountability Act) privacy of medical records
GLB (Gramm-Leach-Bliley) privacy of financial information
Database Security Breach Act (CA)
DMCA) Digital Millennium Copyright Act - RIAA empowerment act
the university technology environment
no university firewall
  that would be silly
some school firewalls
some internal firewalls
good router ACLs (in some places)
mostly switches
reasonable clue in most official IT groups
near software monoculture on non-student desktops
mixed server picture
the players
cA staff
school staff
undergrad students
grad students
tenants
researchers
faculty
my task
  (until Larry changes the culture)
get the schools to think they came up with security and privacy efforts
  use laws as sticks when enthusiasm fades
get buy-in on guidelines
too much
  posture, pontificate & cajole
too little
  “you must”
but I knew what I was getting into
  this bed was already on fire
thanks & have a good lunch