

Security Planning for the Future

**Stan Yagi
Assistant CIO,
Information Technology**

Background

- Scope of the problem is national / international
- No easy fixes
- The costs are high -- the risks are even higher
- Social / cultural issues are complex

Developing a Strategy

- **Chancellor's Committee on Cybersecurity and Faculty**
- **CITES working groups**
 - threat analysis
 - cultural feasibility
 - technical feasibility

Goals

- Provide an overview of the problem and the complexities
- Identify specific measures to address the problem including cost estimates
- Communicate an overall strategy to the campus and continue discussion
- Seek funding for implementation

Threat Analysis

- Virus v. Worm
- Scope of vulnerabilities increasing at alarming rates
- An effective, comprehensive defense plan requires continuing threat analysis capabilities
- Barriers to threat analysis:
 - Lack of data
 - Lack of expertise and standard practice
 - Lack of organizational focus/ownership
 - **Lack of common standard for “acceptable risk”**

Solutions

- Advice on tools and how to develop common standards
- Need to collect appropriate data

Cultural Feasibility

- Input from campus stakeholder / advisory groups (*CCSP, ITAB, SITAB, Senate IT, Committee on Cybersecurity and Faculty*)
- Responsibility for solutions is also multi-layered:
 - CITES & Office of the CIO
 - Department Head who often delegates to dept IT
 - Individual Faculty and Staff
 - Students
- Critical participation by local IT Professionals
 - Align efforts with unit mission and work

Solution

- Education, Education, Education

Technical Feasibility

- No single technology will solve the problem
- Must adopt a multi-layer approach
 - Central Services
 - Departmental Services
 - Desktop systems

Technical Feasibility

- Central Services Solutions
 - Threat analysis
 - Email relays: Virus and spam prevention
 - Campus firewall
 - Patch management
 - Intrusion detection
 - Network Registry services
 - Security awareness training programs

Technical Feasibility

- Department Services Solutions
 - Threat analysis
 - Patch management
 - Switch-based access control lists
 - Intrusion prevention
 - Anti-virus services

Technical Feasibility

- Desktop Systems Solutions
 - Patch management
 - Anti-virus services

Budget

Service	New One-Time (\$1000s)	New Recurring (\$1000s)
Access Control Lists	25	12
Firewall	0	40
Intrusion Prevention	155	24
Traffic Flow Tracking	19	17
Desktop Verification invest	51	11
Email anti-virus/anti-spam	414	266
Desktop anti-virus	150	85
Security Awareness Training	65	25
Patch Management	422	179
Threat Analysis	264	129

What do we get if we don't act?

- Increased vulnerability to the hundreds of new threats each month
- Possible chaos
- Probable loss of data
- Probable loss of productivity
- Possible loss of institutional reputation

How does this change the campus landscape?

- More tools for local administrators
- Fewer threats at departmental level
- More emphasis on adherence to campus policies
- Increased use of push technologies, particularly for unmanaged systems

Conclusion

- The campus IT environment is reflecting significant change across the world
- Multi-layered approach is essential
- Multi-layered approach requires partnership across units
- Need solid relationships and substantial resources to address threats

Next Steps

- Talk with us today about this
- Send email with your comments to cites-feedback@uiuc.edu
- Talk with your department head in support of increased IT security