

COMBINING POLICY, PRACTICE, AND TECHNOLOGY TO ARCHITECT LAYERED NETWORK SECURITY AT UMBI

Mansur Hasib

Director of Information Technology, UMBI
EDUCAUSE 2005 Presentation



UMB
I

UNIVERSITY OF MARYLAND
BIOTECHNOLOGY INSTITUTE



THE NEED FOR SECURITY

- How Much is Enough?
- What Will You Secure?
- The Security Layers: People, Perimeter Entry Points, Connections Between Locations, Hosts, Information Stores, Exit Points



PROCESS

- Gather Requirements
- Define Goals
- Develop a Plan
- Prioritize
- Implement in Priority Order as Funds Become Available
- Gage Success

UMBI

- One of 13 USM Institutions
- Comprises of Center for Advanced Research in Biotechnology (CARB, Rockville), Center of Marine Biotechnology (COMB, Baltimore), Medical Biotechnology Center (MBC, Baltimore), Institute of Human Virology (IHV, Baltimore), and Center for Biosystems Research (CBR, College Park)



REQUIREMENTS

- External Requirements – Legal, State, Regulatory Bodies, Audit
- Internal Requirements – Geography, Desired Performance, Culture, Business Needs, Core Business Hours



GOALS

- Functional Compatibility with State IT Policy
- Encrypted Network Communications
- Layers of Security
- No Loss of Business Functionality
- No Perceptible Loss of Speed
- As Automated as Possible



IMPLEMENTATION

- Develop Security Policies (will guide what is implemented)
- Define the Layers for Security Implementation (policy will guide)
- Develop a Funding Plan
- Prioritize the Implementation (funding plan will guide)



UMBI MODEL

- Network Security Program – defines our user behavior and responsibilities:
<http://www.umbi.umd.edu/computing/secpolr.html>
- Perimeter Security – Firewalls, Router Access Lists, NAT
- Site to Site Encryption
- Secure Administration Tools and Practices

UMBI MODEL - continued

- Operating System Security:
<http://www.nsa.gov/ia/index.cfm>
- Patch Management
- Workstation Level Security:
Automated Patch Management,
Automated Virus Checking and
Updates, Spyware checking,
Workstation Firewalls



UMBI MODEL - continued

- Mail Security: Open Relay Prevention, Virus Checking, Content Blocking, Spam Control
- Dial-in Security: Authentication, Placement Outside Firewall
- Home Users: Education, Controlled Distribution of Access, VPN
- Intrusion Detection and Prevention



INCIDENT RESPONSE PLAN

- Establishes a Response Pattern
- Allows Faster Responses
- Produces Documentation
- Educates IT Staff
- Improves Security
- Example Incident Response Plan:
<http://www.umbi.umd.edu/~hasib/irp.pdf>



RESULTS

- Reduced Downtime
- Increased Staff Productivity
- Successful Audits
- Satisfied Users
- Satisfied Management



CONCLUSION

- UMBI's Implementation of a Layered Security Architecture Addressed: People, Perimeter Entry Points, Connections Between Locations, Hosts, Information Stores, Exit Points