

**Hampton Roads
Cyber Security
Awareness Conference**

October 21, 2008

Managing Information Security Threats in Higher Education

Wallace C. Arnold, Presenter

On today's campus, Information Technology supports, enhances and extends:

- Teaching and learning
- Research
- Business management and Administration
- Indispensable contacts with

students
faculty
donors
vendors
granting agencies

staff
alumni
applicants
public



**IT is
Complex
and
Costly**

VULNERABILITY

As the University reaches out.....the world
reaches back



**The Threat to
Higher Ed
Secure
Operations**

Threats to Information Security

- Denying access to networks
- Compromising or changing data affecting integrity
- Theft of data, from.....
 - Insiders (authorized users)
 - Organized crime groups
 - Terrorist organizations
 - Foreign governments

INSIDERS

Students

Staff

Faculty

Outside Contractors & Vendors

Strategic Partners

70% of unauthorized access cases by insiders or others who are authorized.

Insider breaches cost \$10 billion annually.

Insiders corrupt valuable network resources.

Difficulty in tracking access privileges.

COMMON CAUSES OF INSIDER ATTACKS

- **Poor morale**
- **Fluctuating economy**
- **Weak internal safeguards**
- **Overly trusting work environment**

MULTIPLE SOLUTIONS

- Security policies
- Educating and training inside users
- Increasing security beyond firewall and password

Security Policies Should Address.....

- **Managing network resources.**
- **Granting students, staff, faculty and others access.**
- **Handling security breaches.**
- **Password requirements.**
- **User and system administrative authority.**
- **Antivirus authority.**
- **Handling proprietary information.**
- **Physical security.**

Education & Training

- **Start with hiring and new relationships.**
 - **Non-disclosure agreement.**
 - **Computer use agreement.**
- **Network security procedures.**
- **Information handling procedures.**
- **Organizational security policies.**
- **Dangers of allowing others access to one's personal account.**

- **Mishandling passwords.**
- **Storage of passwords.**
- **E-mail hackers**
- **Instant messaging and file sharing.**
- **Employee behavior.**
- **Incident response teams.**

Hardware and Software Security Measures

- Internal auditing.
- Intrusion detection systems.
- Network level access controls.
- Internet filtering applications.
- Password protection software.
- Virtual private networks (VPNs)
- Encryption tools.
- Biometric devices.
- Hardening computers and servers.

- **Don't open security holes with configuration changes.**
- **Don't mistakenly give users administrator level privileges.**
- **Only give necessary level of access when new application is installed.**
- **Access for students, staff and faculty by internally segmenting work environment.**
- **Virtual local area networks (VLANs).**

CONCLUSION

- **Soft target for criminal intent.**
- **Illegally riding a university network.**
- **Increasing demand for greater access.**
- **Balancing need for access against security risk.**
- **No single solution.**
- **Evolving solutions against evolving cyber threats.**
- **Strong leadership from top-down.**