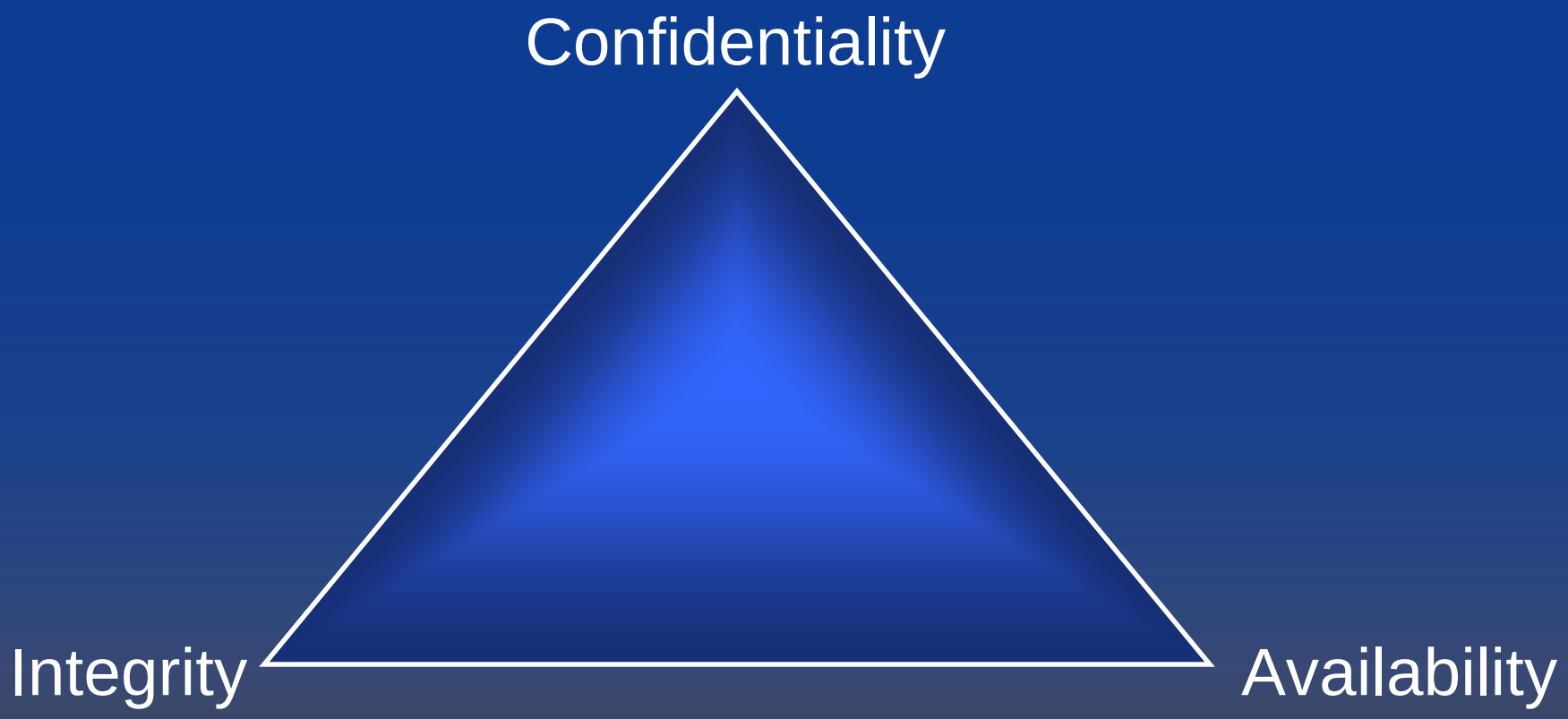
Network Security

Wallace Wilhoite, CISSP
wmw2@cdc.gov

SAFER • HEALTHIER • PEOPLE™

CIA Triad



The Threats

- Hackers & Script Kiddies
- Misconfigurations
- Unprotected points of entry
- OS Vulnerabilities
- Computer viruses
- Advertisers/Spam

Threat Response Components

- Policies & Practices
- Perimeter defenses
- Vulnerability analysis
- Strong authentication practices
- File and session encryption
- Virus & spam protection
- Knowledge transfer
- Incident response handling

Policies & Practices

- No Policy = Everything Allowed
- Supported by top management
- Consistent with acceptable IT practices
- Reasonable & enforceable
- Best security practices

Perimeter Defense

- Routers
- Firewalls
- Intrusion detection systems
- Content vectoring

Vulnerability Analysis

- External & internal network scanning
- System/Network auditing
- Phone line sweeping
- Independent validation & verification

Strong User Authentication

- Develop and enforce authentication standards
- Periodic password strength analysis
- Multiple factor authentication to access secure services

File and Session Encryption

- Secure Sockets Layer (SSL)
- VPN encryption
- File encryption
- Data remanance

Virus & Spam Protection

- Layered approach is essential
- Obscure file types stripped at gateways
- Enhance information exchange and sources
- Hoaxes
- Computer virus alert system
- Anti-Spam technologies and practices

Knowledge Transfer

- Systems Administration & Network Security Institute
- NIST
- Carnegie Mellon
- Extreme Hacking Training
- Security awareness
- Attend/present at IT security seminars & conferences

SANS Institute online
A Cooperative Education & Research Organization

NIST
National Institute of Standards and Technology

Carnegie Mellon
Software Engineering Institute
CERT® Coordination Center

Incident Response Handling

- Develop incident response plan
- Create incident response team and exercise plan
- Participate in FBI **INFRAGARD** program
- Guidance available from NIST, Carnegie Mellon and SANS

Summary

- Effective network security is achieved through a combination of best practices, policies and technologies. No single practice, policy or technology can stand alone to provide all layers of protection.

Security Resources

- CDC BT Technical Guidance

  bttech@cdc.gov

  http://www.cdc.gov/cic/functions-specs/email.htm
- NIST Computer Security Resource Center

  http://csrc.nist.gov/
- Carnegie Mellon

  http://www.cert.org/
- Systems Administration and Network Security (SANS) http://www.sans.org

Network Security

Wallace Wilhoite, CISSP
wmw2@cdc.gov

SAFER • HEALTHIER • PEOPLE™