

Community
Network 2002 **NOBODY
LEFT BEHIND**



Security 101: Proactive Security "Facing 21st Century Technology"

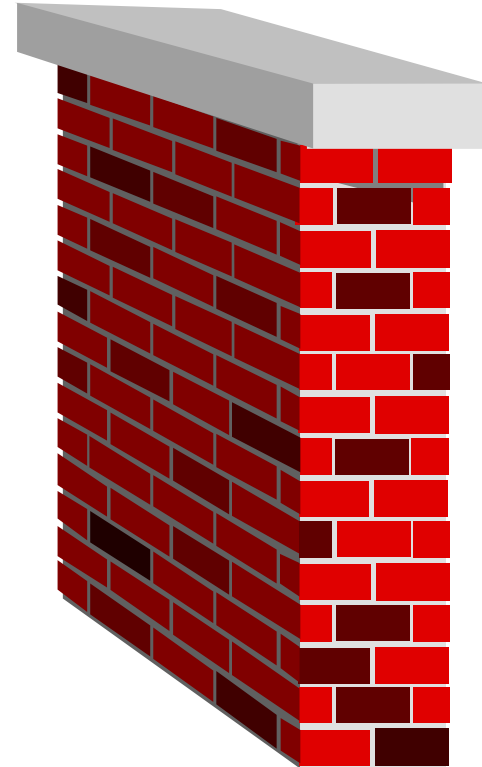
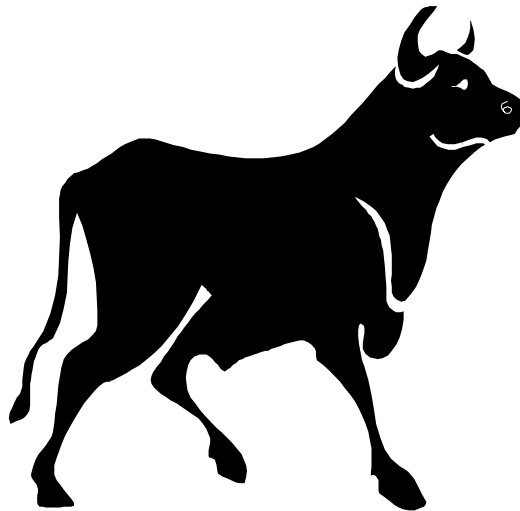
Chancery SMS – Win School®

All Users 1-3



Welcome!

Mike Houser



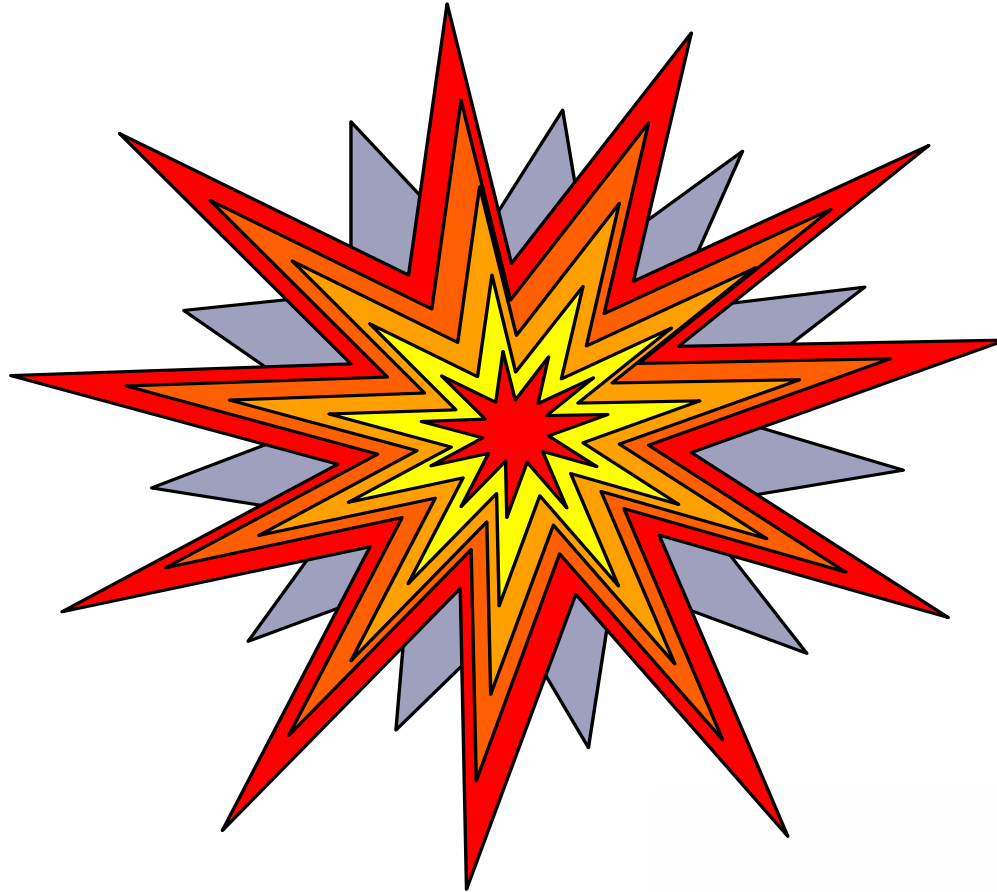
Community
Network 2002 **NOBODY
LEFT BEHIND**





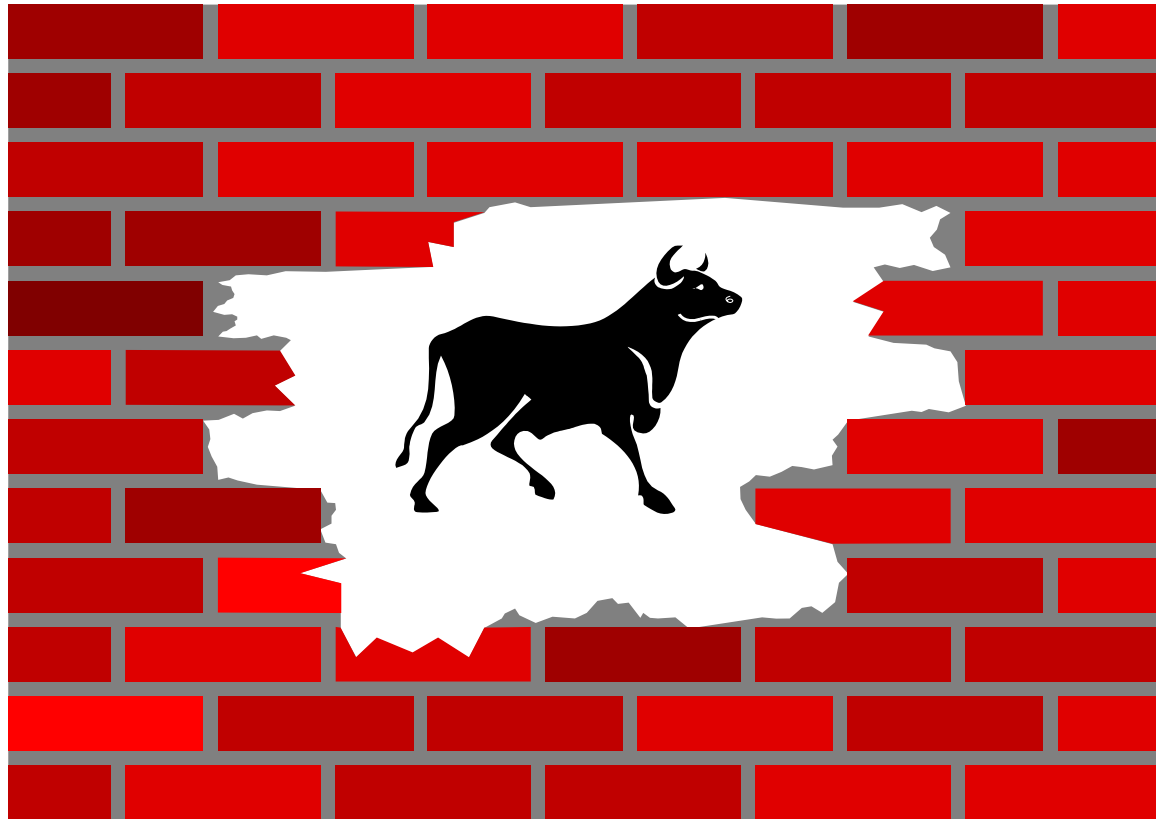
Community
Network 2002 **NOBODY
LEFT BEHIND**





Community
Network 2002 **NOBODY
LEFT BEHIND**



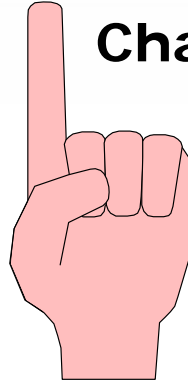


Community
Network 2002 **NOBODY
LEFT BEHIND**





Chancery Recommendations "Q & D"



Getting familiar with your guides

- The "B-Word"
- Users, passwords, & user access
- eClass considerations

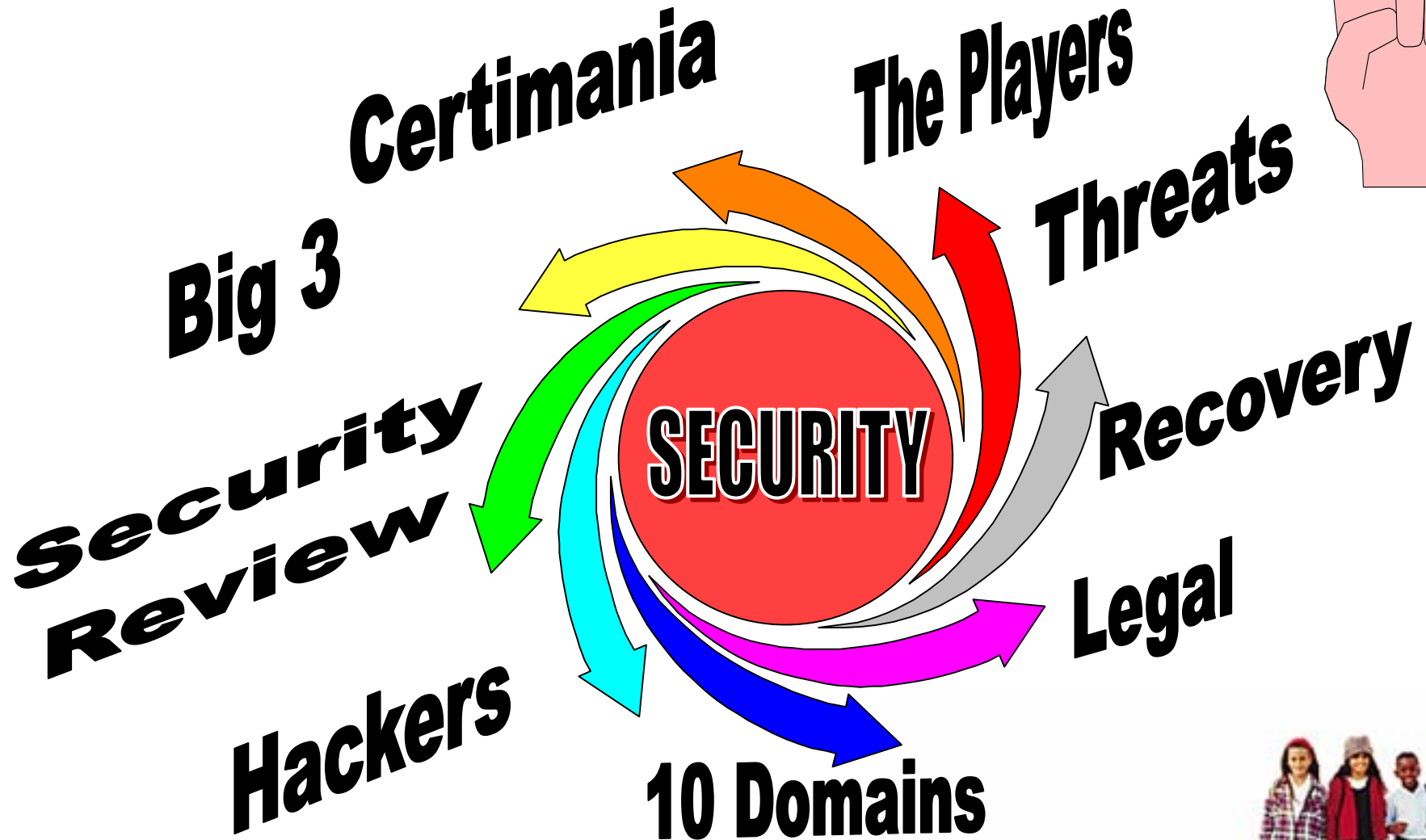
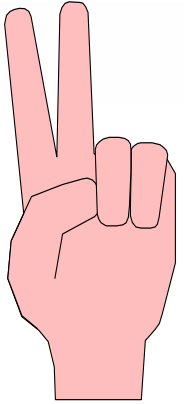
(Specific network issues are beyond our scope)



Community
Network 2002 **NOBODY
LEFT BEHIND**

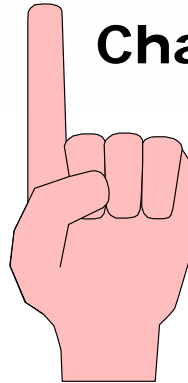


Facing 21st Century Security Issues



Community
Network 2002 **NOBODY
LEFT BEHIND**





Chancery Recommendations "Q & D"

Getting familiar with your guides

System Administrator Guide

- Configuration files
 - Workstations
 - Servers
 - Maintenance





Getting familiar with your guides

System Administrator Guide

- The "B-word"
 - Methods
 - Rotations
 - Storage (off site)
 - Testing backups





Getting familiar with your guides

System Administrator Guide

School Setup Guide

- Users, passwords & access
- Tips & tricks





Chancery Recommendations "Q & D"

When first you begin:

1. ADMINISTRATOR

ID field -- probably 0 -- up to 7 digits

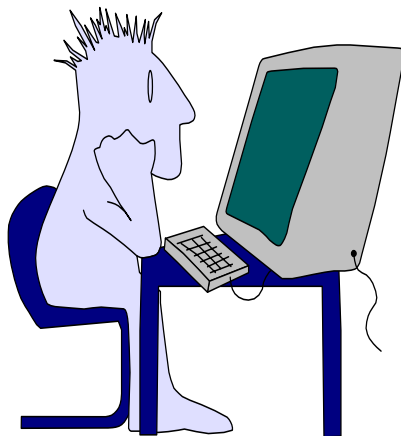
Password field -- up to 7 letters or numbers (case sensitive)

Uncheck "Ignore Passwords and Access Level settings"

2. OTHER ACCOUNT for routine use

3. BACK-DOOR ACCOUNT with ADMINISTRATIVE rights

4. TEMPLATE ACCOUNTS by user types



Community
Network 2002 **NOBODY
LEFT BEHIND**





Chancery Recommendations "Q & D"

User ID & Password

USER ID can be up to 7 digits.

USER ID must be unique.

USER PASSWORD can be up to 7 letters or numbers.

USER PASSWORDS are case sensitive.



Community
Network 2002 **NOBODY
LEFT BEHIND**



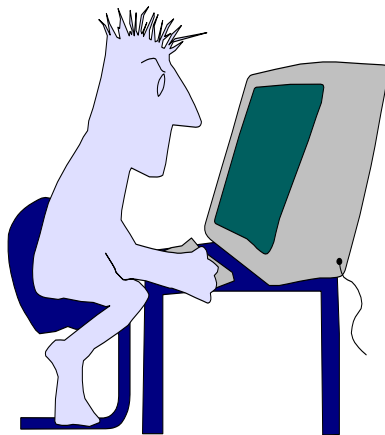


Chancery Recommendations "Q & D"

Check Point #1

Passwords should not be easy to guess.

Users should not share IDs and Passwords.



Community
Network 2002 **NOBODY
LEFT BEHIND**





Chancery Recommendations "Q & D"

Check Point #2

Know your rights!!

None

View

Edit

Change only

Multi-User View

Multi-User Edit



Community
Network 2002 **NOBODY
LEFT BEHIND**





Chancery Recommendations "Q & D"

HOW TO BEGIN

1. Determine exactly what the user will be expected to do.
Ask questions.
2. Go to the computer.
 - "Quiet" time!
 - 15 minutes per unique user!
3. Assign the security.
 - Decide whether to copy* a template with adjustments.
 - Assign ID & Password.
 - Assign minimum level of rights. (Need to know!)
4. Test each ID and Password with assigned rights.
5. Validate ID, password, and rights with each user.

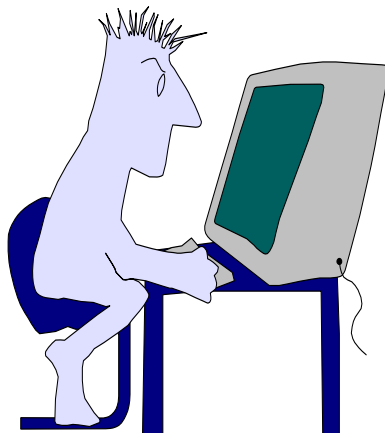




Chancery Recommendations "Q & D"

Check Point #3

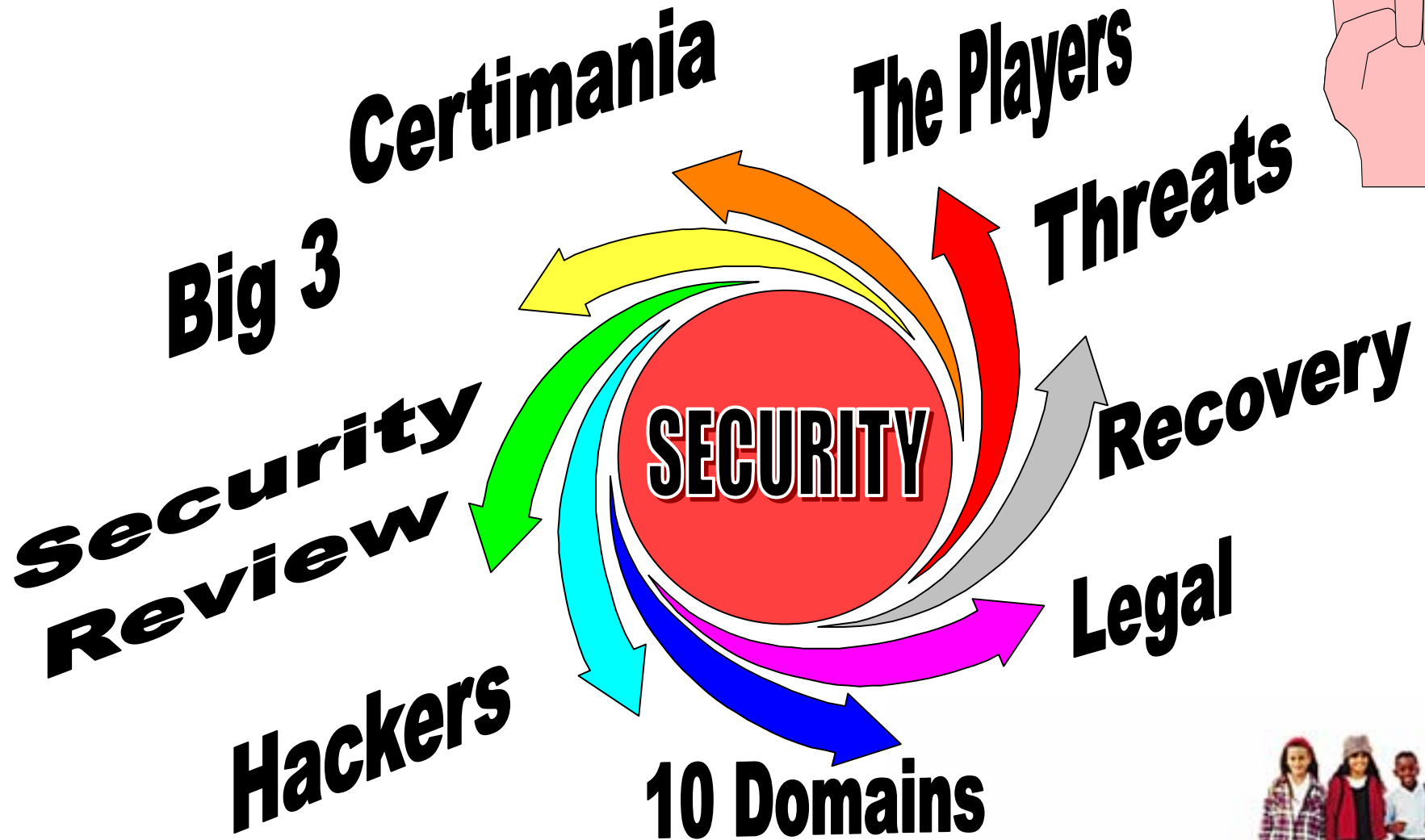
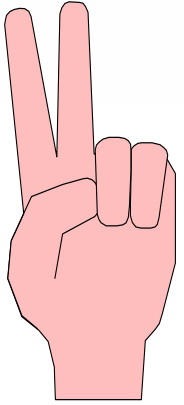
Set an eClass Grades password for school administrators.



Community
Network 2002 **NOBODY
LEFT BEHIND**



Facing 21st Century Security Issues

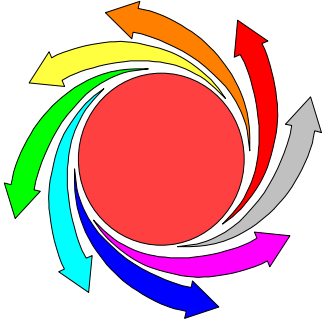


Community
Network 2002 **NOBODY
LEFT BEHIND**





Facing 21st Century Security Issues



**“You deserve to be hacked,
and by the way,
you will be.”**

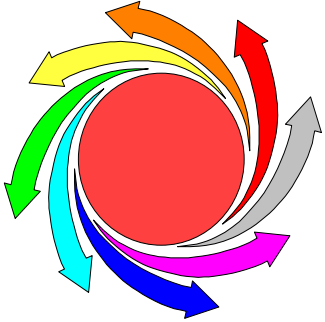
(Source: Unknown but probably a HACKER!)

Community
Network 2002 **NOBODY
LEFT BEHIND**

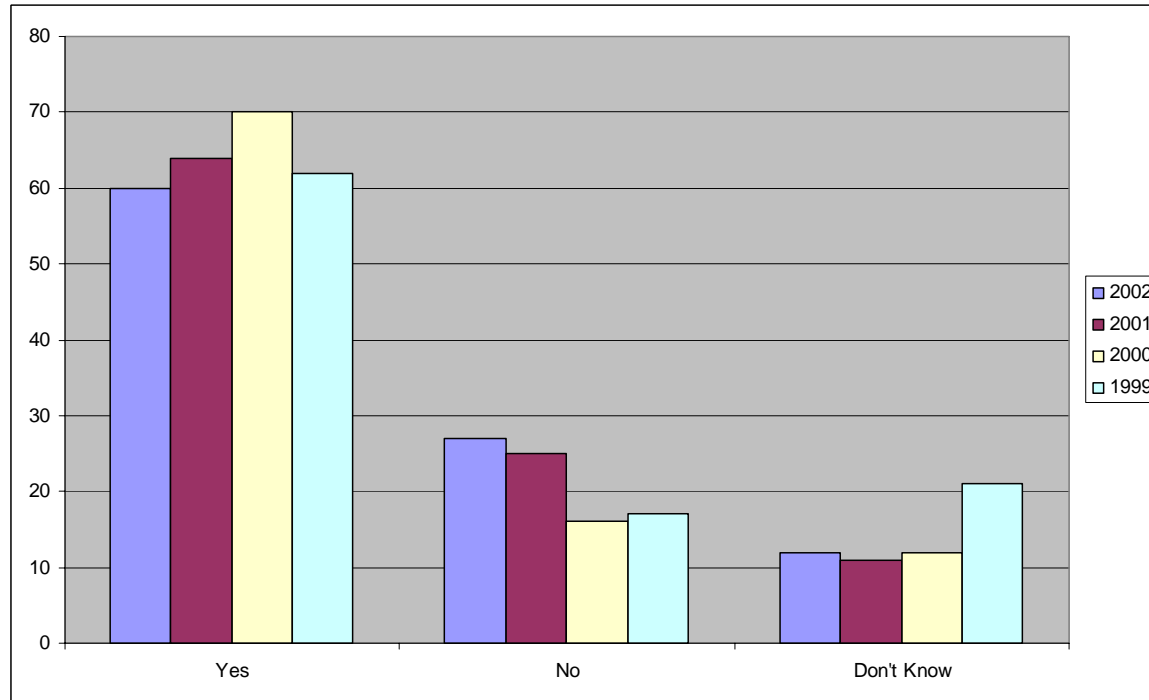




Facing 21st Century Security Issues

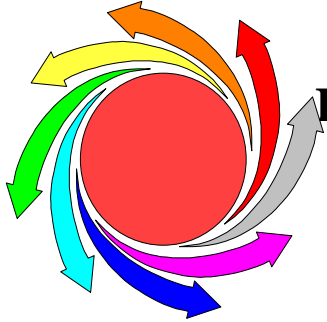


Unauthorized Use of Computer Systems Within the Last 12 Months CSI/FBI 2002 Computer Crime and Security Survey

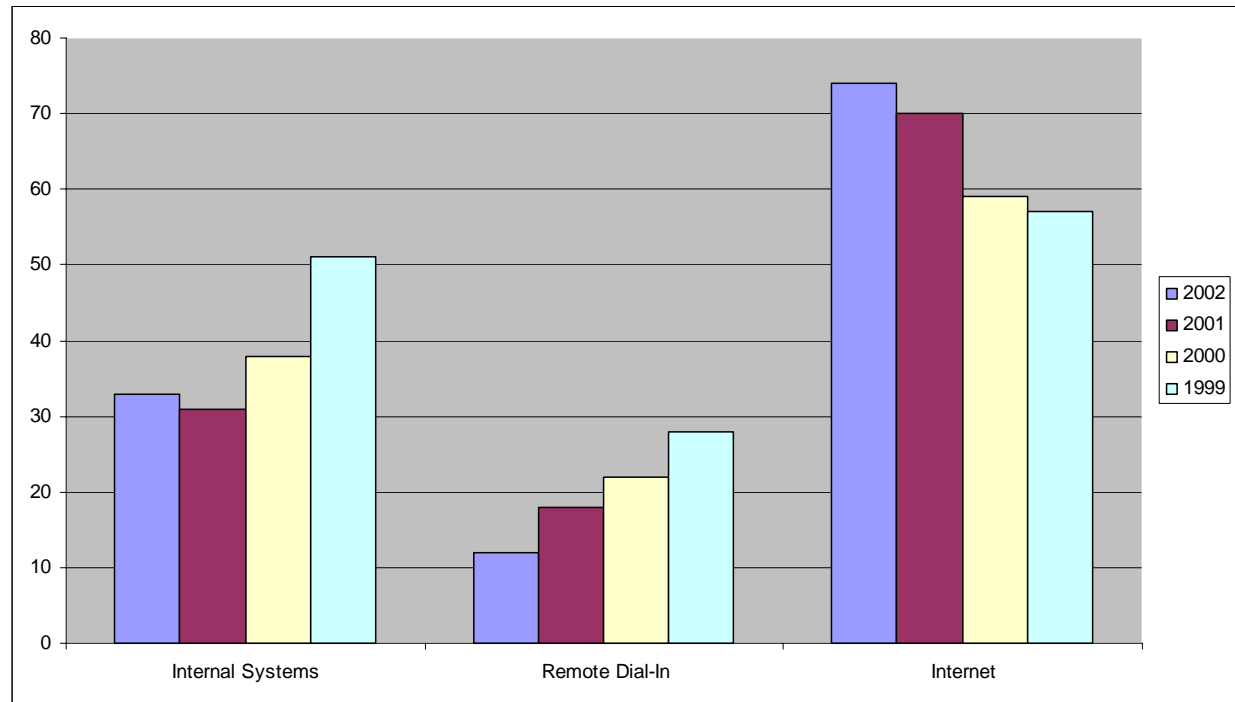




Facing 21st Century Security Issues

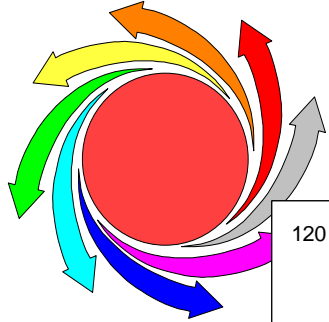


Internet Connection is Increasingly Cited as Frequent Point of Attack CSI/FBI 2002 Computer Crime and Security Survey

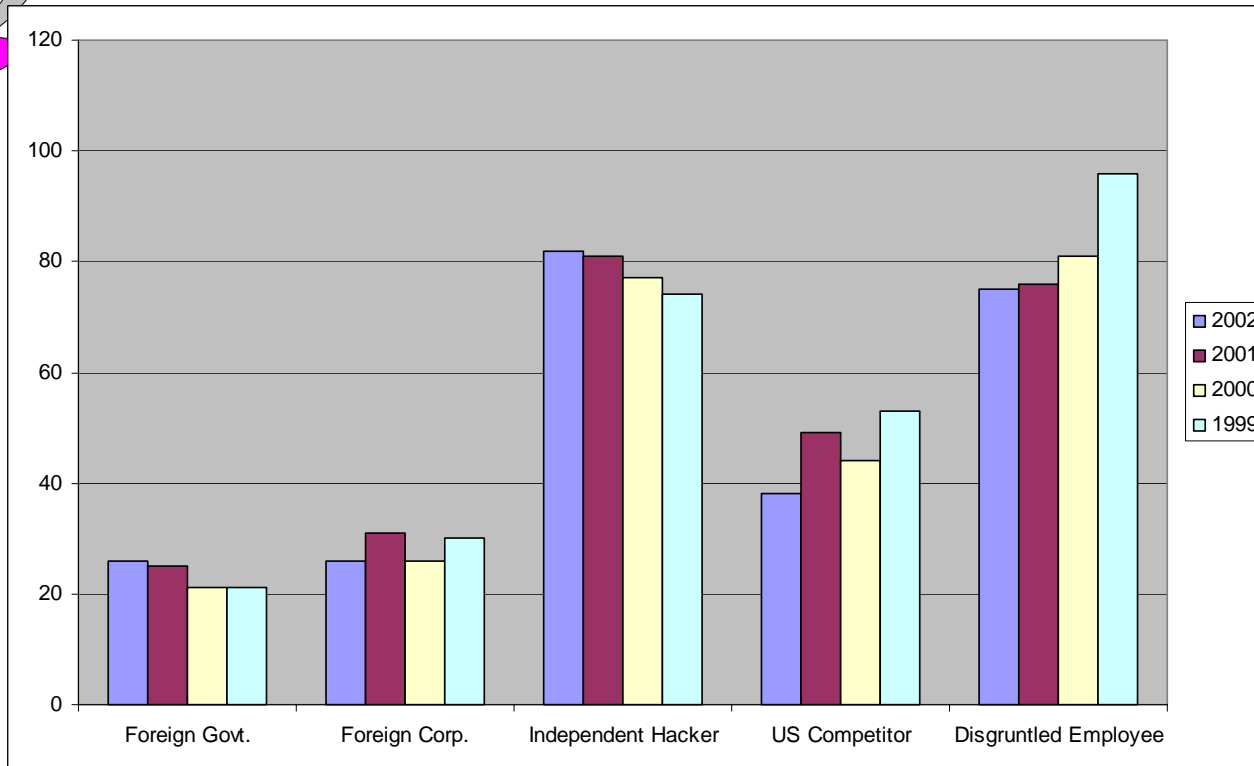




Facing 21st Century Security Issues



Likely Sources of Attack
CSI/FBI 2002 Computer Crime and Security Survey

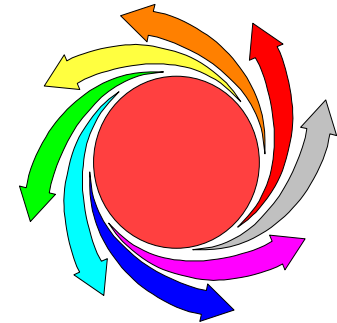


Facing 21st Century Security Issues

Types of Attack or Misuse Detected in the Last 12 Months (%)

CSI/FBI 2002 Computer Crime and Security Survey

| | |
|----------------------------------|----|
| Denial of Service | 40 |
| Laptop | 55 |
| Active Wiretap | 1 |
| Telecom Fraud | 9 |
| Unauthorized Access by Insiders | 38 |
| Virus | 85 |
| Financial Fraud | 12 |
| Insider Abuse of Net Access | 78 |
| System Penetration | 40 |
| Telecom Eavesdropping | 6 |
| Sabotage | 8 |
| Theft of Proprietary Information | 20 |

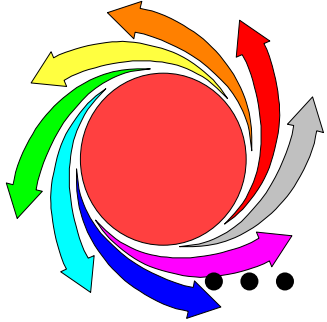


Community
Network 2002 **NOBODY
LEFT BEHIND**





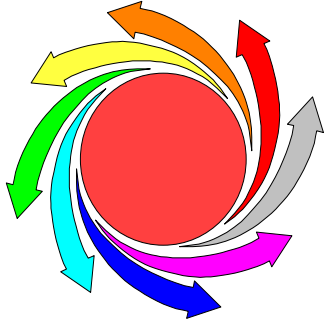
Facing 21st Century Security Issues



... and speaking of **HACKERS** ...

- Glamorized
- Tools of the trade
- Activities
 - Footprinting
 - Port scanning
 - Lurking, invading, stealing, & destroying

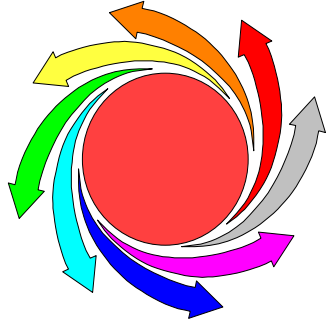




URGENCY!

- **SECURITY**
 - Mile-wide topic!
 - Chunking!
- DISA (free resources)
- Certification
 - 10 Associations/Agencies
 - CISSP (ISC)2
 - Security+ (CompTIA)

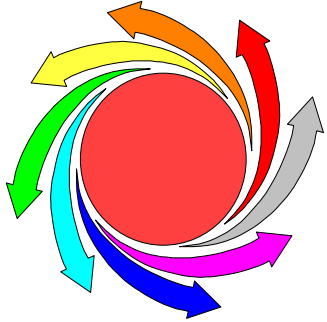




The Players

- **Hardware**
- **Software**
- **Peopleware**
- **Data**
- **Other**





Reality Check

\$ = Hardware

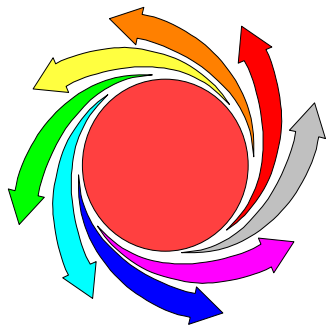
\$ = Software

\$\$\$\$? = Peopleware

\$\$\$\$\$???? = Data

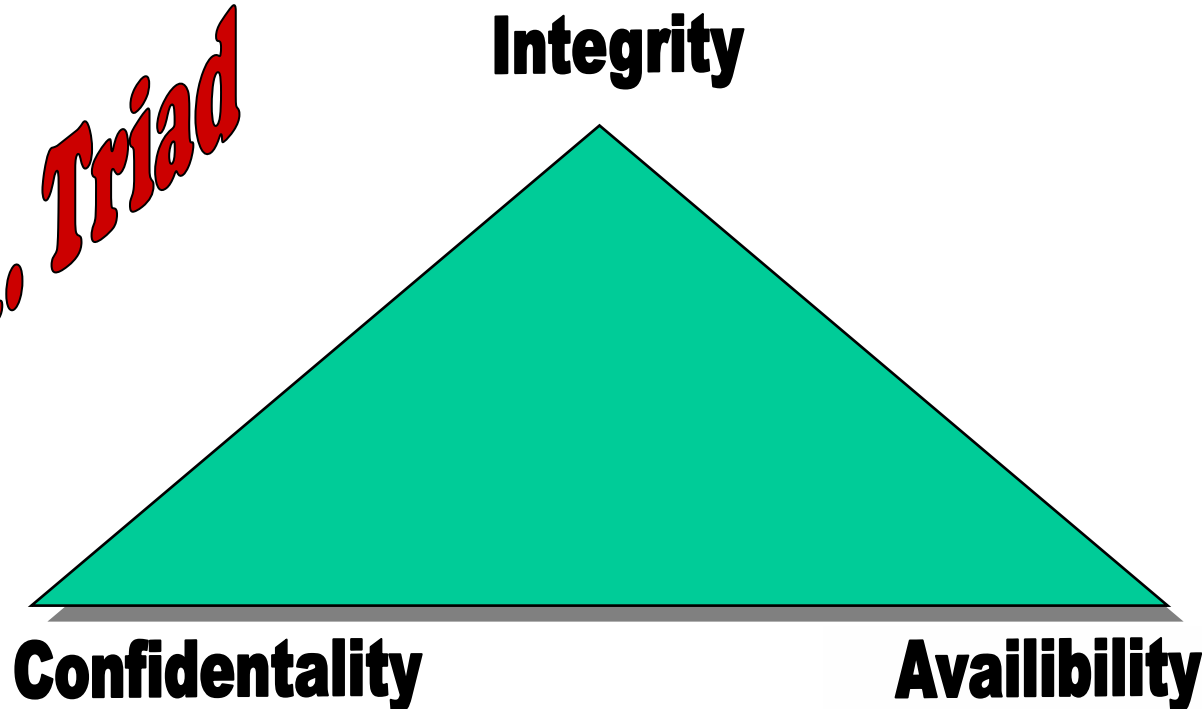
?????????? = Other

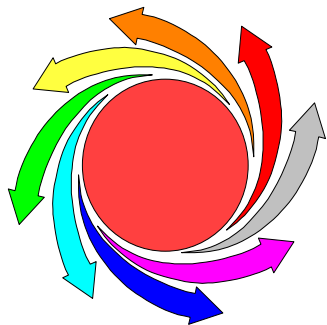




Qualities of Information

C.I.A. Triad





Reverse of C.I.A.

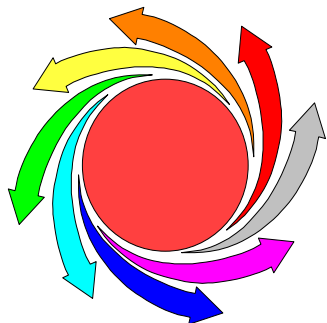
D.A.D. Triad

Alteration

Disclosure

Destruction





Mitigating Risk

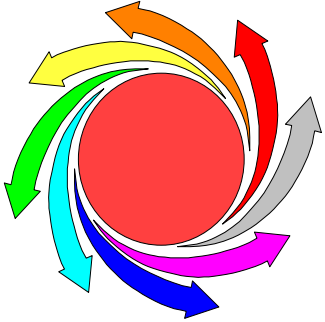
HOW MUCH RISK CAN YOU TOLERATE???

“It’s important to remember that the risk to an enterprise can never be totally eliminated – that would entail ceasing operations.”

“Risk Mitigation means finding out what level of risk the enterprise can safely tolerate and still continue to function effectively.”

(Source: The CISSP Prep Guide)



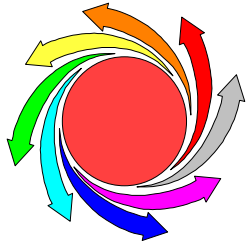


Assessing Risks

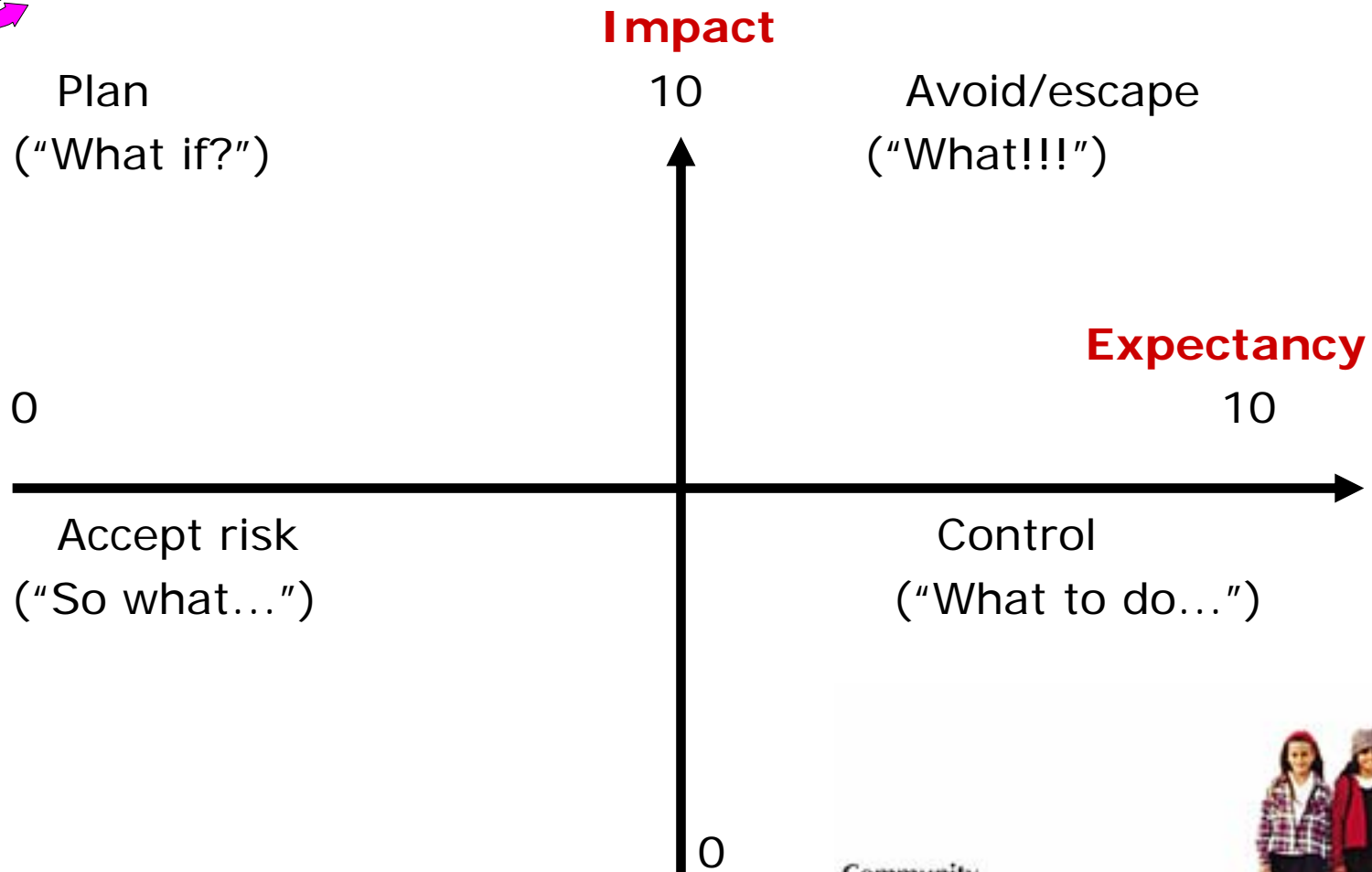
Doing the math!!!

$$\text{RISK} = \text{Threats} + \\ \text{Vulnerabilities} + \\ \text{Asset Value}$$



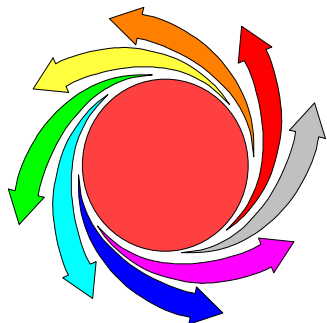


Policy Decisions





Facing 21st Century Security Issues



Classroom

Countering the Dangers!

- Organizational procedures
- Physical security
- Document security
- Personnel security
- Hardware security
- Software security
- Network security
- Continuity planning and disaster recovery
- Security awareness



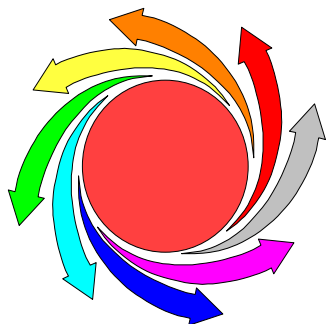


Facing 21st Century Security Issues

Countering the Dangers!

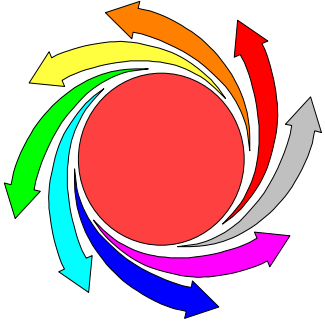
Ten Domains of Computer Security

- Security Management Practices
- Access Control Systems
- Telecommunications & Network Security
- Cryptography
- Security Architecture and Models
- Operations Security
- Applications & Systems Development
- Business Continuity Planning and Disaster Recovery Planning
- Law, Investigation, and Ethics
- Physical Security

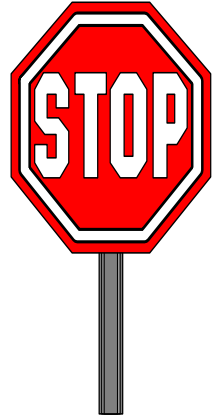


Countering the Dangers!





Emerging Idea

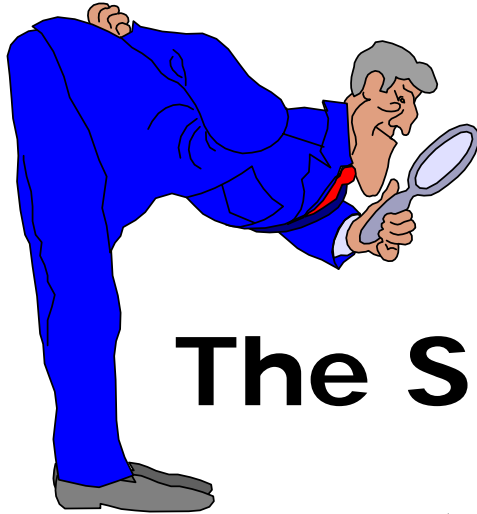


- **SECURITY REVIEW**
 - We are all in this together!
 - We all own the problem!
 - We need the support of all the players!
- What we expect, we must all inspect!



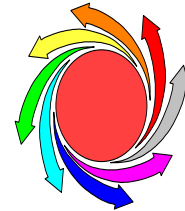
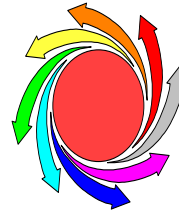
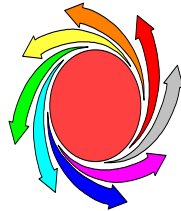
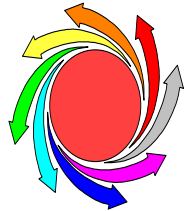


Facing 21st Century Security Issues



The SECURITY REVIEW

"Work In Progress"



Community
Network 2002 **NOBODY
LEFT BEHIND**





Answers to Your Questions



Community
Network 2002 **NOBODY
LEFT BEHIND**



- Free Resources from **DISA**
 - <http://iase.disa.mil/>
- Free PDF file from **Computer Security Institute** [A MUST READ!!!]
 - "Computer Security Issues & Trends:
2002 CSI/FBI Computer Crime and Security Review"
 - <http://www.gocsi.com>
- Consideration for IT decision-makers
 - <http://microsoft.com/security>
 - Microsoft® Security Toolkit
 - Microsoft® Baseline Security Analyzer
- CISSP® Information
 - <http://www.isc2.org>
- Security+® Information
 - <http://www.comptia.org>
- Just for fun
 - The Cuckoo's Egg (Clifford Stoll)
- Other Printed Resources
 - Commonsense Computer Security (McGraw-Hill)
 - The CISSP Prep Guide (Wiley Pub.)
 - Hacking Exposed (McGraw-Hill)
 - Know Your Enemy (Addison-Wesley)
- Chancery's Technical Support 1-800-688-9939
- Chancery's Support web site support.chancery.com
- Michael S. Houser "Mike"
Email = DrMHouser@yahoo.com

All handouts, tip sheets, & more are available on Mike's personal website at:
<http://mikehsr.tripod.com>



Auf Wiedersehen!

Thank You



Community
Network 2002 **NOBODY
LEFT BEHIND**

