



Strategies, Solutions and Innovations for Technology Leaders
April 29, 2004 • Itasca, IL

Security

Desktop to Server

Joe Huber
Director of Information Systems
Greenwood Schools, IN
joehuber@iupui.edu

Produced by:
TECHNOLOGY
 **LEARNING**



A Few Stats.

- **Most intrusions originate inside the network** (ISO, International Organization of Standards)
- **80% to 90% of all intrusions due to unpatched software** (CERT, Computer Emergency Readiness Team)
- **Cost 19.7 billion dollars in 2002** (ISTS, Institute for Security Technology Studies)
- **One day tech support for every eMail user** (NIST, National Institute for Standards in Technology)

Produced by:





Cause of the Problem!

- Over the last few years K12 schools have spent millions of dollars to develop high speed data networks.
- Few resources (\$\$ and personal) to spend on security.
- Availability and ease of use of current hacking tools.



CoSN Calculator

<http://classroomtco.cosn.org/>

Strategies, Solutions and Innovations for Technology Leaders
 April 29, 2004 · Itasca, IL

Technology Staffing Guidelines Worksheet

District:	Sample School			
	Computers, etc	1,940.00	/500	3.88
A	Major responsibilities	10.50	/5	2.10
B	Software	22,138.00	/5000	4.43
C	Users	1,170.25	/1000	1.17
D	Teachers	197.00	/150	1.31
E	Web	0.05		0.05
F	Telephone	0.38		0.38
G	Video	0.03		0.03
H	Other	0.02		0.02
I	Management	1.25		1.25
J			Total A-J	14.62
	Outsourcing	0.30		(0.30)
K			Total A-K	14.32
	Environment	-	add 10-20%	-
L	Low priority	-	subtract 0-25%	-
M	High priority	25%	add 0-25%	3.58
N				
Total staffing				17.90

B	Major responsibilities	Days/week
	List each major task with the estimated	
	Windows 95	1.00
	Windows NT	0.50
	Network Admin	3.00
	Email system	0.50
	Administrative	1.50
	MAC	1.50
	Mcafee virus	1.00
	Web servers	1.50
		10.5

C	Software	# software titles	# computers	Total Software
	staff or admin use	10.00		
	teacher use	10.00	98.00	980
	elementary student use	31.00	155.00	1,550
	middle/high school use	10.00	443.00	13,733
	other	5.00	446.00	4,460
			283.00	1,415
			1425	22,138

D	Users	# of users	Weighted Users
	50-100%/day	53.00	
	10-50%/day	1,072.00	53.00
	Occasional	3,325.00	536.00
	Total Users	3450	581.25
			1,170.25



Likelihood Definitions

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.



Likelihood Analysis

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised, the following factors must be considered:

- Threat-source motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current controls



Impact Analysis

The adverse impact of a security event can be described in terms of loss or degradation of the following security goals:

- Loss of Confidentiality
- Loss of Availability
- Loss of Integrity



Impact Definitions

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede and organization's mission or reputation; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede and organizations mission or reputation; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission or reputation.

Produced by:





Risk Determination

- Risk Determination assess the level of risk to the IT system
- The determination of risk for a particular threat/vulnerability pair can be expressed as a function of the following:
 - The likelihood of a given threat-source attempting to exercise a given vulnerability
 - The magnitude of the impact should a threat-source successfully exercise the vulnerability
 - The adequacy of existing security controls for reducing or eliminating risk



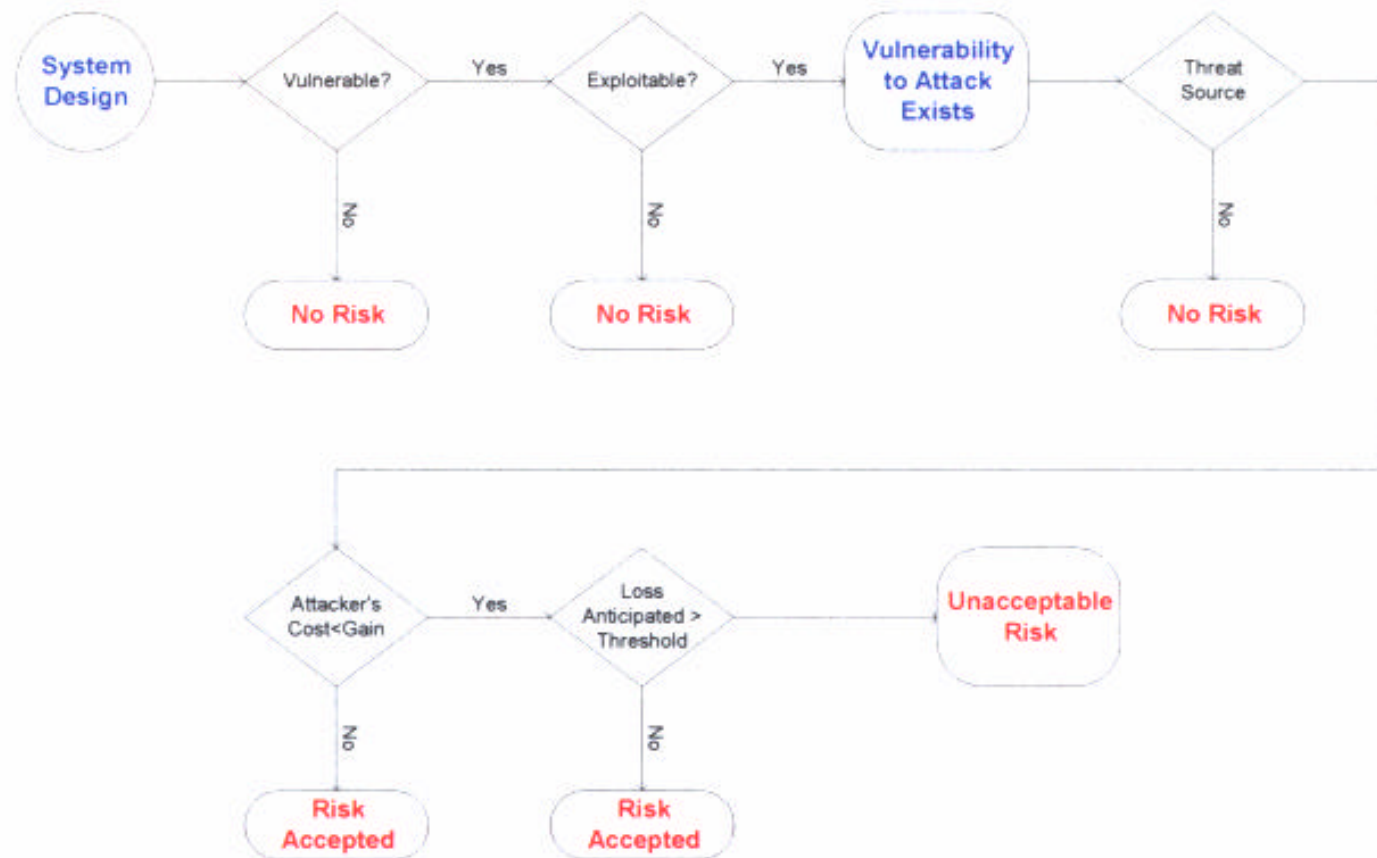
Risk Level Matrix

Threat Likelihood	Impact		
	Low (1)	Medium (5)	High (10)
High (10)	Low $10 \times 1 = 10$	Medium $10 \times 5 = 50$	High $10 \times 10 = 100$
Medium (5)	Low $5 \times 1 = 5$	Medium $5 \times 5 = 25$	Medium $5 \times 10 = 50$
Low (1)	Low $1 \times 1 = 1$	Low $1 \times 5 = 5$	Low $1 \times 10 = 10$

Risk Scale: High = 100, Medium = 11 to 99, Low = 1 to 10



Risk Mitigation Strategy





Operational Risk Assessment ISO 177799

- A comprehensive set of controls comprising best practices in information security
- It is intended to serve as a single reference point for identifying a range of controls needed for most situations in information security.
- An international recognized generic information security standard or policy



Operational Risk Assessment ISO 177799 What is included?

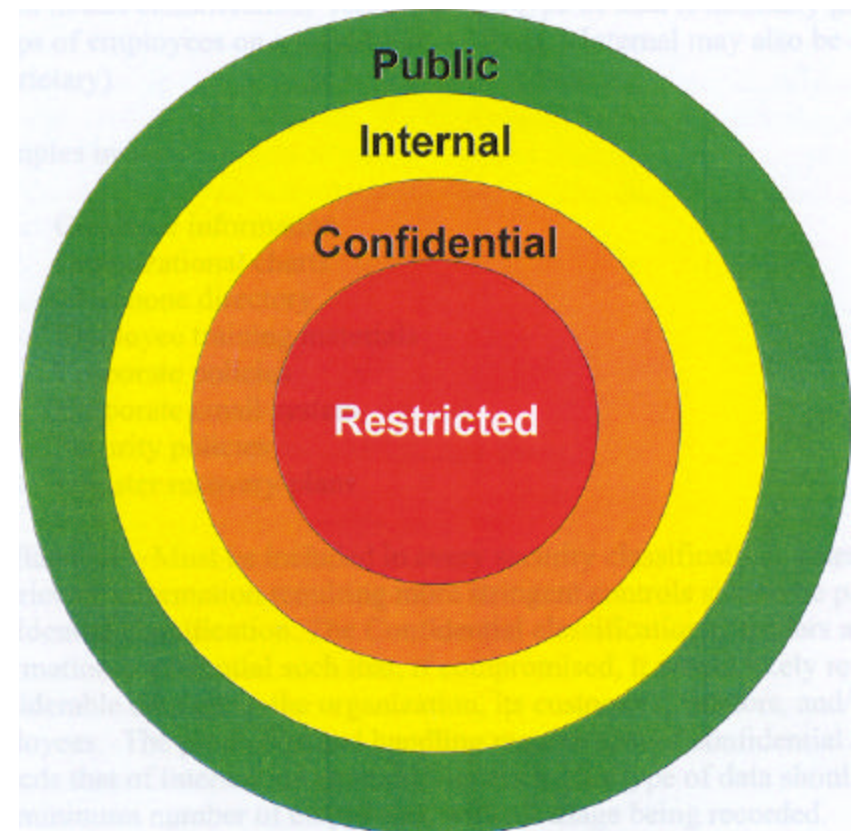
- Business Continuity Planning
- System access control
- System development and maintenance
- Physical and environmental security
- Compliance
- Personnel Security
- Communication & Operations Management
- Asset Classification and Control
- Security Policy

Produced by:



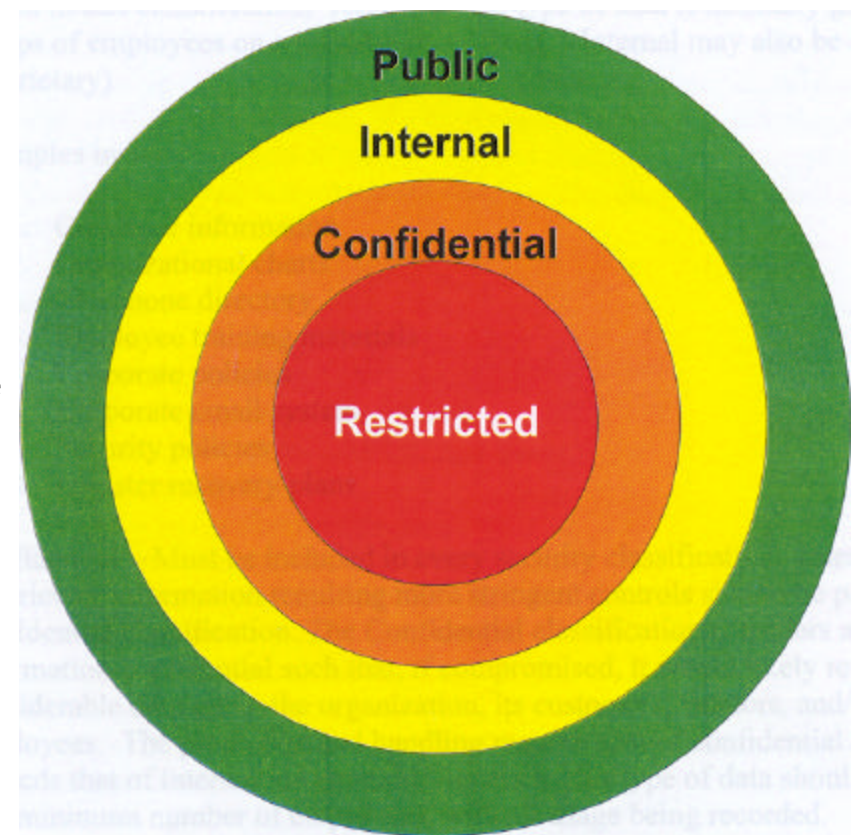
Security Classification Model

- **Public**
Information not specific to any individual or project (School web pages)
- **Internal**
Information where if unauthorized disclosure, modification, or destruction COULD have adverse effects on the organization (student network application that hold student data, data analysis programs)



Security Classification Model

- **Confidential**
Internal or proprietary information (Student academic and health data, staff evaluation)
- **Restricted**
Information if compromised the result would likely cause severe financial, legal, regulatory or reputation damage (Counselor or social worker records on students, individual student free and reduced lunch information)





User Access Management

- Explicit and enforceable A.U.P
- A.U.P. MUST be reviewed and signed every year.
- Change Passwords frequently (every 30 days maximum) or use Biometric devices (U-R-U by digital **Persona**)
- Programs That **Limit** users access and/or ability to make changes

DeepFreeze and FreezeX

Policies and ZenWorks not enough

- Active Directory
- Port Access
- Mac address and/or IP address access

Produced by:





Free Tools

- **Find MP3 files on your LAN**
<http://www.globalshareware.com/Mp3-Audio/MP3-Search-Tools/2-Find-MP3.htm>
http://www.shareup.com/LAN_Find-download-8231.html
- **UPDATE!, UPDATE!, UPDATE!**
S.U.S Server (software update services)
<http://www.microsoft.com/windowsserversystem/us/default.mspx>



Free Tools

- **Microsoft Baseline Security Analyzer**
<http://www.microsoft.com/technet/security/tools/mbsahome.mspx>
- **IIS Lockdown Tool**
<http://www.microsoft.com/technet/security/tools/locktool.mspx>
- **Uptime command-line tool**
<http://www.microsoft.com/downloads/details.aspx?FamilyID=285348E1-9AC2-45A1-A467-6968397E6C73&displaylang=en>



Free Tools

- **Windows Server Resource Tool Kit**

<http://www.microsoft.com/downloads/details.aspx?FamilyID=9D467A69-57FF-4AE7-96EE-B18C4790CFFD&displaylang=en>

- **Net diagnostics tool**

<http://www.microsoft.com/downloads/details.aspx?FamilyID=aae64b62-27c0-4523-8af9-66a968a8c942&displaylang=en>



Free Tools

- **Center for Internet Security Scoring Tool**

<http://www.cisecurity.org/>

- **Nessus**

<http://www.nessus.org/>

Powerful, up-to-date and easy to use remote security scanner. Requires Unix computer (can be installed on new Mac OS).