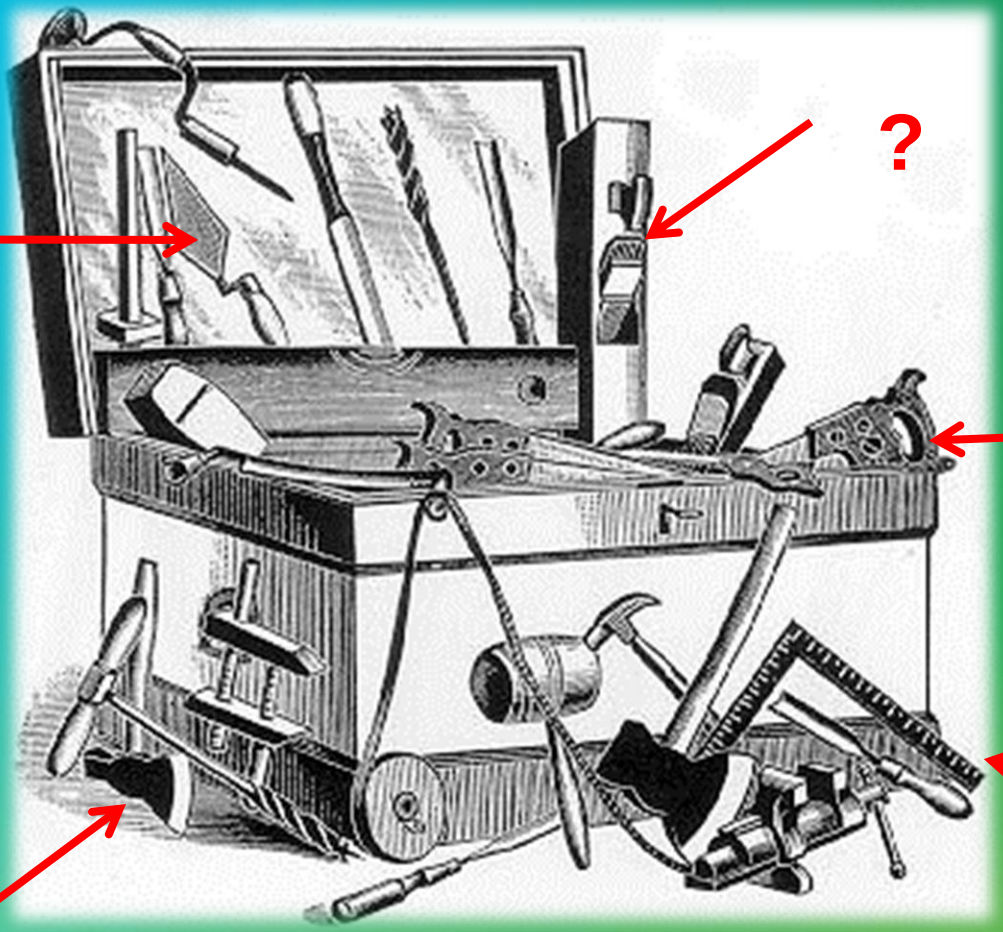
SANS AppSec 2012

Panel: How to Get the Most Out of Your Tools

Michele D. Guel
Distinguished IT Engineer & Senior Security Architect/Advisor/Evangelist
Communication and Collaboration IT, Cisco

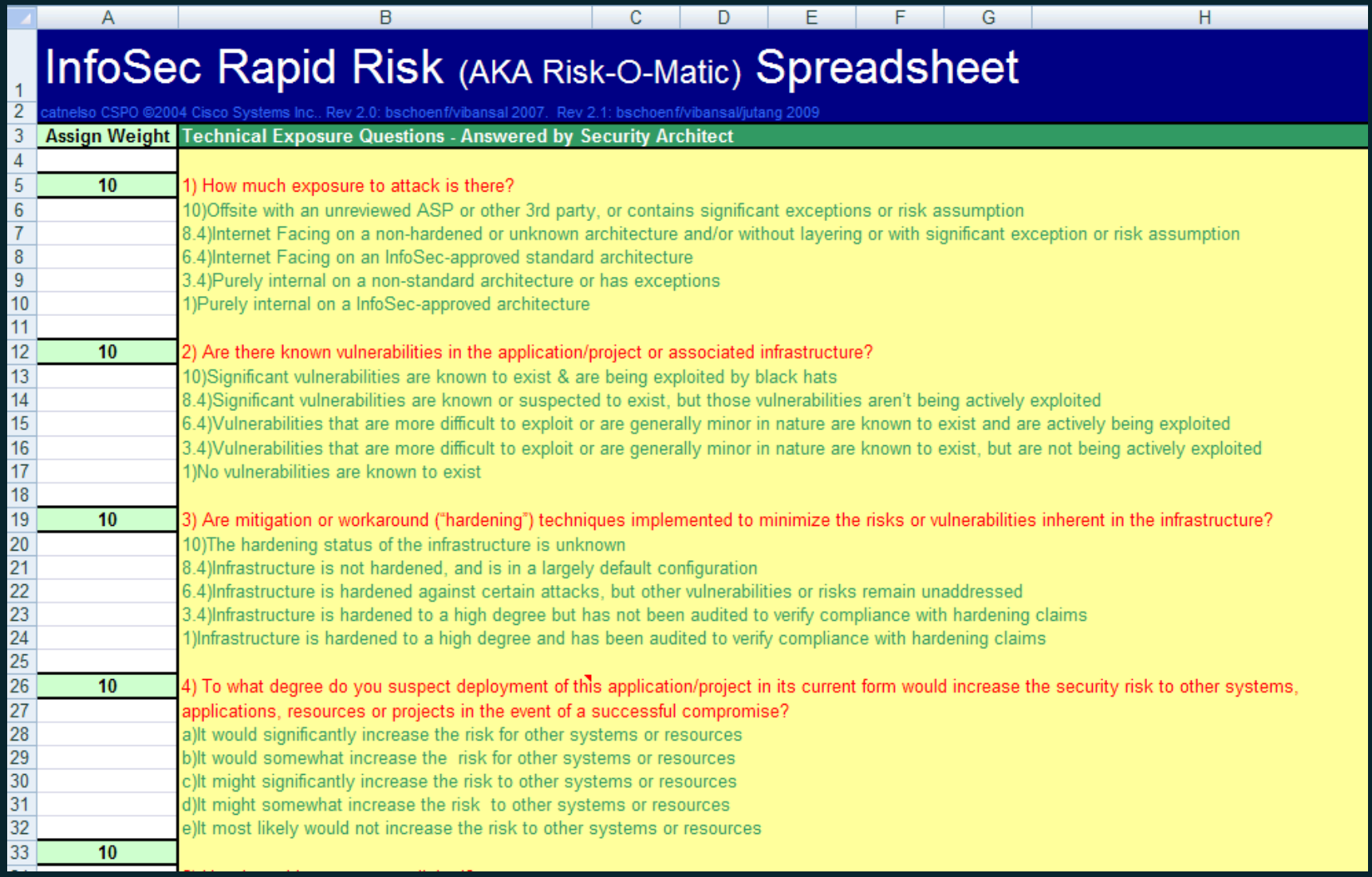
Who am I

- 16 year veteran of Cisco
- Founding member of what is now the Corporate Security Programs Office
- Have worked in multiple facets of information security for 23 years
- Was part of an “experiment” at Cisco to move security people out of corporate group – great learning's
- Total security geek and very passionate
- Current focus is How to Bake in Security and codify the practice



What is my Favorite Tool?

The Rapid Risk Assessment Tool

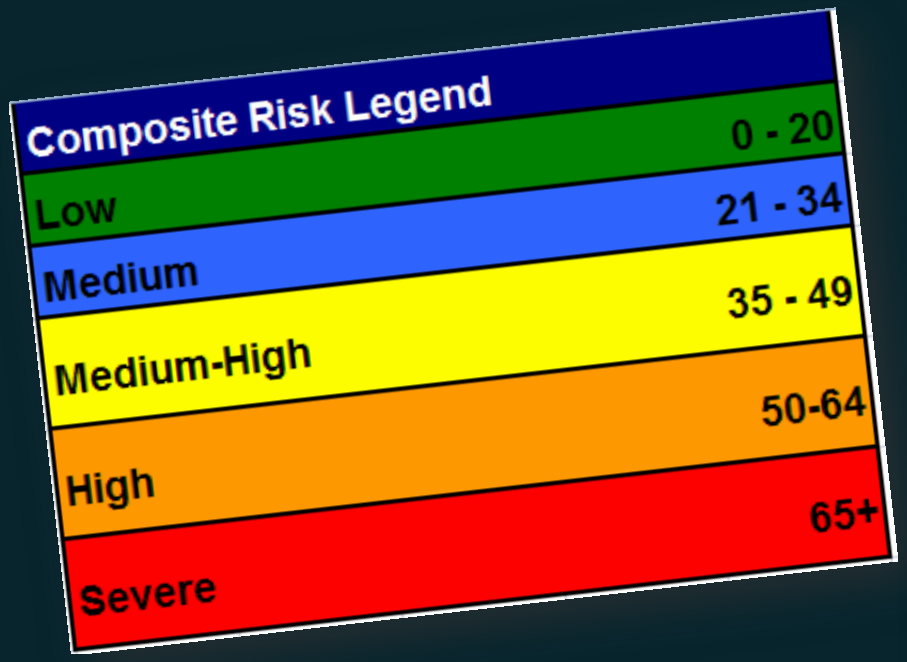


	A	B
1	InfoSec Rapid Risk (AKA Risk-O-Matic) Spreadsheet	
2	catnelso CSPO ©2004 Cisco Systems Inc.. Rev 2.0: bschoenf/vibansal 2007. Rev 2.1: bschoenf/vibansal/jutang 2009	
3	**Assign Weight**	**Technical Exposure Questions - Answered by Security Architect**
4		
5	**10**	1) How much exposure to attack is there?
6		10)Offsite with an unreviewed ASP or other 3rd party, or contains significant exceptions or risk assumption
7		8.4)Internet Facing on a non-hardened or unknown architecture and/or without layering or with significant exception or risk assumption
8		6.4)Internet Facing on an InfoSec-approved standard architecture
9		3.4)Purely internal on a non-standard architecture or has exceptions
10		1)Purely internal on a InfoSec-approved architecture
11		
12	**10**	2) Are there known vulnerabilities in the application/project or associated infrastructure?
13		10)Significant vulnerabilities are known to exist & are being exploited by black hats
14		8.4)Significant vulnerabilities are known or suspected to exist, but those vulnerabilities aren't being actively exploited
15		6.4)Vulnerabilities that are more difficult to exploit or are generally minor in nature are known to exist and are actively being exploited
16		3.4)Vulnerabilities that are more difficult to exploit or are generally minor in nature are known to exist, but are not being actively exploited
17		1)No vulnerabilities are known to exist
18		
19	**10**	3) Are mitigation or workaround ("hardening") techniques implemented to minimize the risks or vulnerabilities inherent in the infrastructure?
20		10)The hardening status of the infrastructure is unknown
21		8.4)Infrastructure is not hardened, and is in a largely default configuration
22		6.4)Infrastructure is hardened against certain attacks, but other vulnerabilities or risks remain unaddressed
23		3.4)Infrastructure is hardened to a high degree but has not been audited to verify compliance with hardening claims
24		1)Infrastructure is hardened to a high degree and has been audited to verify compliance with hardening claims
25		
26	**10**	4) To what degree do you suspect deployment of this application/project in its current form would increase the security risk to other systems,
27		applications, resources or projects in the event of a successful compromise?
28		a)It would significantly increase the risk for other systems or resources
29		b)It would somewhat increase the risk for other systems or resources
30		c)It might significantly increase the risk to other systems or resources
31		d)It might somewhat increase the risk to other systems or resources
32		e)It most likely would not increase the risk to other systems or resources
33	**10**	

Why is it My Favorite?

- It's easy to use!
- It takes < 20 minutes
- It smokes out exceptions (to standards)
- Has transformed years of experience into 10 assessment questions
- The answers scale (big or small project)
- It separate business impact from technical exposure
- The project teams "get it"

Scoring is Simple



Cool Colors – LOW Risk

Hot Colors – HIGH Risk

Answer Weight Index	
Answer	Weight to Assign
a	10
b	8.4
c	6.4
d	3.4
e	0

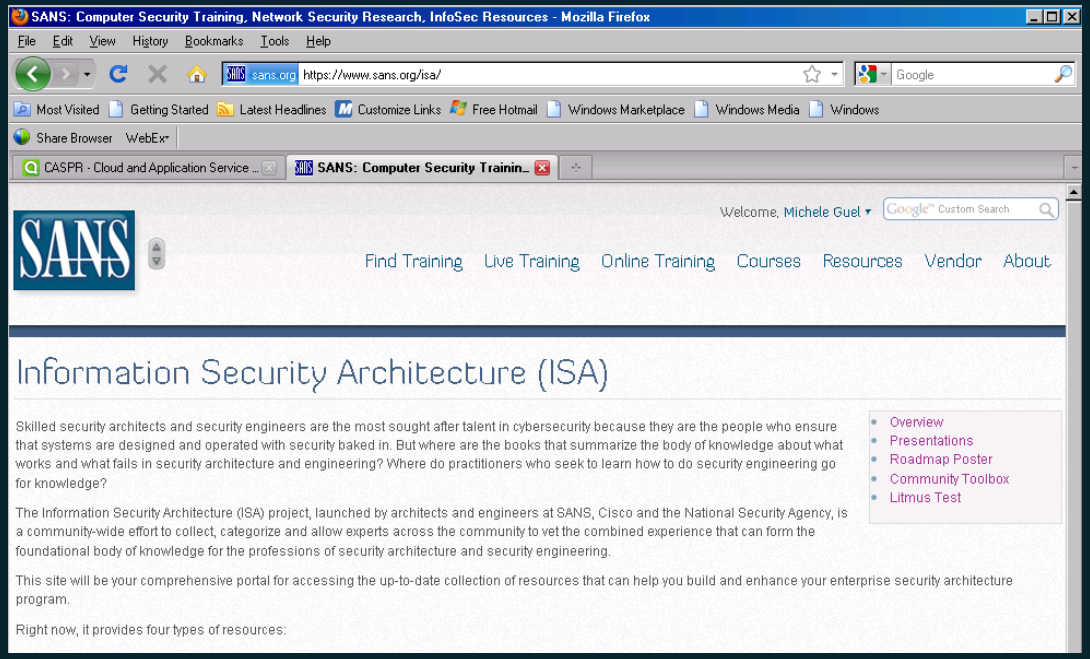
For each question, click on the green highlighted cell next to the question to select the correct wieght from the pull-down menu.
Remember only one weight per question.
The total score will be calculated automatically at the bottom.
Note: The sheet is protected, you can only enter answers in the green cell next to each question.

You Can Assess Twice to Gauge Value

- At first engagement point to assess unknowns
- Before the readiness review to assess effectiveness of engagement

How are security engagements affecting projects?

Where to get the tool?



https://www.sans.org//isa/

Click on “Community Toolbox”
(required sans login)

Thank You!