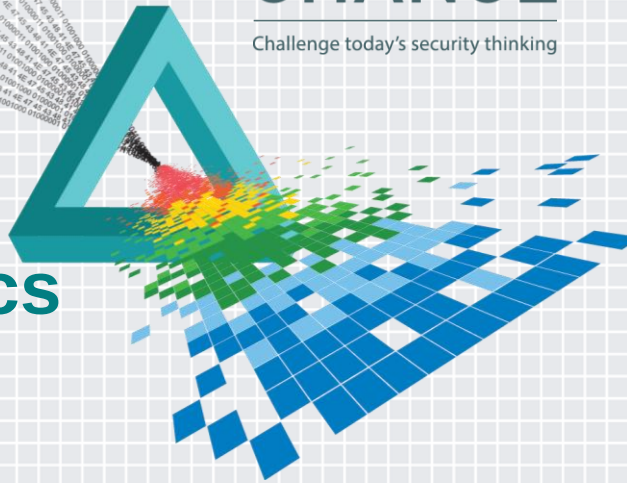
RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking



SESSION ID: CXO-R02

The Truth about Cyber Risk Metrics

Connecting Vulnerabilities to Economics

Scott Borg

U.S. Cyber Consequences Unit

"You can't always get what you want. But if you try sometimes you just might find . . .You get what you need."

What I'm Going to Talk About

Three Wrong Kinds of Risk Metrics

I. The Kind of Risk Metrics People Want (Fantasy Metrics!)

II. The Act-of-Desperation Metrics (Survey Numbers!)

III. Useful Metrics Misrepresented as Risk Metrics (Work Progress)

Two Right Kinds of Risk Metrics (Both Based on Economics)

IV. What a Real Risk Metric Would Look Like (Three Separate Risk Factors)

V. An Easier, Alternative Metric (Attacker Cost)

I. The Kind of Risk Metrics People Want: Fantasy Metrics

Wish list of features (sometimes called the “criteria for a good metric”):

- based on easily available information
- requiring no additional research
- inexpensive to produce
- easy for an automated program to generate
- involving no subjective judgments
- capable of being updated in a matter of minutes

(Regularly supplied by unscrupulous or deluded vendors)

II. The Act-of-Desperation Metrics: Survey Numbers

If you don't know what's going on or how to proceed . . .

1) Poll *other* people who don't know what's going on or how to proceed

2) Report the numbers

3) Repeat the polls at different times to generate trend lines

4) Dress the numbers up in graphs and bar charts

5) Draw whatever conclusions you like!

(A major part of the annual cyber security reports produced by vendors)

III. Useful Metrics Misrepresented as Risk Metrics: Work Progress Metrics

- Metrics for the progress in work devoted to reducing vulnerabilities
- Measured by the percent to which each task on a vulnerability check list has been carried out:
  - Default security settings changed
  - Unused connection options disabled
  - Patches & updates applied
  - Firewall configurations updated
  - Strong passwords used
  - Increases in privileges logged & reviewed
  - Privileges revoked after people have left their jobs
  - Laptops with auto-play options turned off
  - Etc., etc. . . .

(III). Selling Work Progress Metrics as "Risk Reduction" Metrics

Security tool venders often put "risk metrics" into their products that:

1) Assign a "criticality factor" to each of the security tasks
2) Multiply the percentage of finished tasks times their criticality factors
3) Add up the total
4) Divide by the sum of the criticality factors
5) Present the result as a "risk reduction metric"

$$\frac{(\%\ \text{Completed}_1 \times \text{Criticality Factor}_1) + (\%\ \text{Completed}_2 \times \text{Criticality Factor}_2) + \ldots}{\text{Criticality Factor}_1 + \text{Criticality Factor}_2 + \ldots}$$

(III). Why Treating Work Progress Metrics as Risk Reduction Metrics Doesn't Work

1) There is *no* reduction in risk until enough vulnerabilities have been removed so that the attacker can no longer find the remaining ones.

2) Many vulnerabilities are in systems that are relatively unimportant or that no one would want to attack. Others are in systems where an attack could be catastrophic. Work progress metrics can't tell the difference.

3) There is no such thing as a general "criticality factor" for one type of system or component. Different industries and even different companies have different systems that are critical.

4) Vulnerabilities need to be analyzed collectively, in terms of paths, not one-by-one.

(III). The Dangers of Treating Work Progress Metrics as Risk Reduction Metrics

1) They create an illusion of risk reduction when there is none.

2) They lead to wrong priorities and misplaced efforts.

3) They cause most of the opportunities for stopping an attacker to be neglected, except for penetration.

4) They focus only on vulnerabilities, ignoring the possibilities for reducing threats and consequences.

(III). Cyber-Security "Maturity Levels"

- A kind of higher order work progress metric, grouping security tasks into stages and postponing some until later
- Make people feel better about having bad, ill-conceived security programs

BUT . . .

- A company's needs and priorities will hardly ever correspond closely to a generic sequence of levels
- No need to postpone a genuine risk-based approach, because it can be done iteratively, using whatever information is currently available

IV. What a Real Risk Metric Would Look Like: Three Separate Risk Factors

Threat x Consequence x Vulnerability

= Risk

= Annualized Expected Loss

Threats are not vulnerability exploits!

Consequences are not consequences for information systems!

Vulnerabilities, in this equation, are not attack avenues!

(IV). The Real Risk *Reduction* Metric

Examine the *mechanisms* that generate attacks (Threat), value (Consequence), and attacker success (Vulnerability)! Then calculate:

$Threat_1$ x $Consequence_1$ x $Vulnerability_1$ before risk reduction

minus

$Threat_2$ x $Consequence_2$ x $Vulnerability_2$ after risk reduction

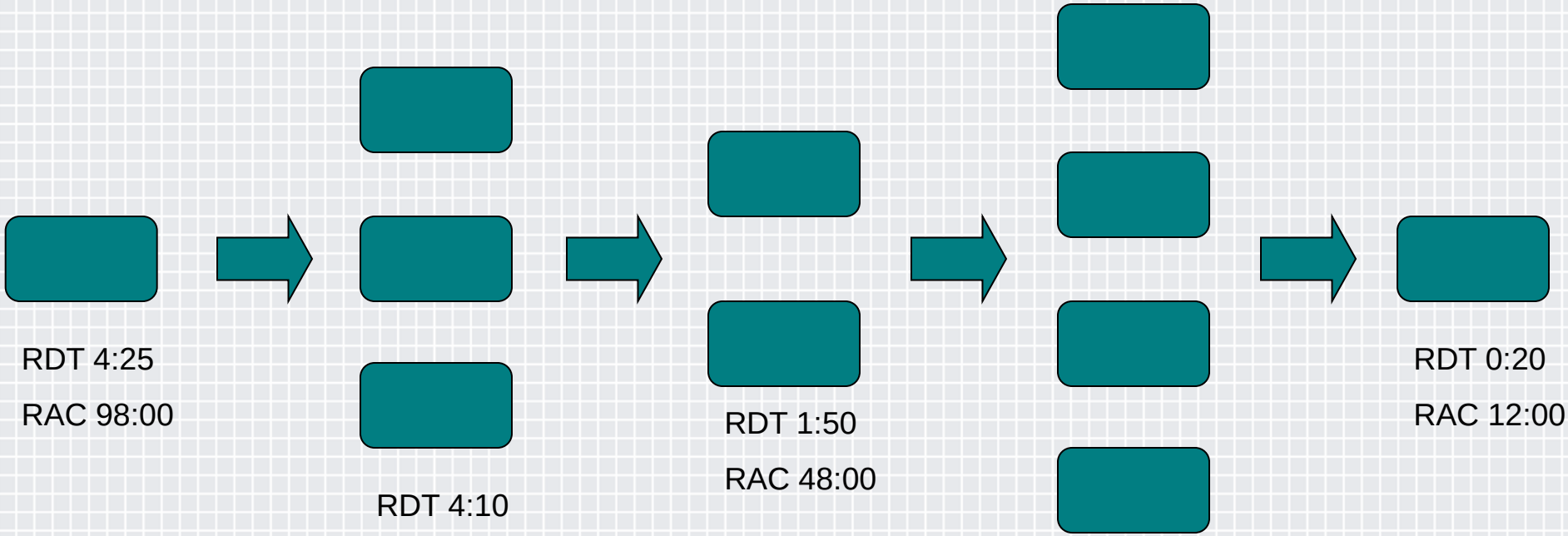
=

Reduction in Risk

=

Reduction in Annualized Expected Loss

(IV). Using Work Flows to Understand Consequences



RDT = Recoverable Down Time, RAC = Recoverable with Added Capacity

(IV). Advantages of a Real Risk Reduction Metric

- Saves security teams from tunnel vision and being blind-sided
- Opens up a far greater range of opportunities for reducing risk
- Translates cyber security into business terms (AEL's, ROI's, etc.)
- Makes security decisions objective, quantitative, and easy to defend (I.e., secures your budget and saves your job if bad things happen)
- Gives cyber security an achievable goal

(IV). Disadvantages of a Real Risk Reduction Metric

- Requires some quantitative knowledge of threats: who is out there, their goals, capabilities, & costs
- Requires some quantitative knowledge of consequences: how and where the organization being defended is creating value, and where its operations could create liabilities

Hence, currently beyond the scope of most cyber-security departments, who are confined to vulnerabilities by their job descriptions and training

V. An Easier, Alternative Metric: Attacker Cost

Instead of trying to reduce your expected losses, you can concentrate on reducing your attacker's gains.

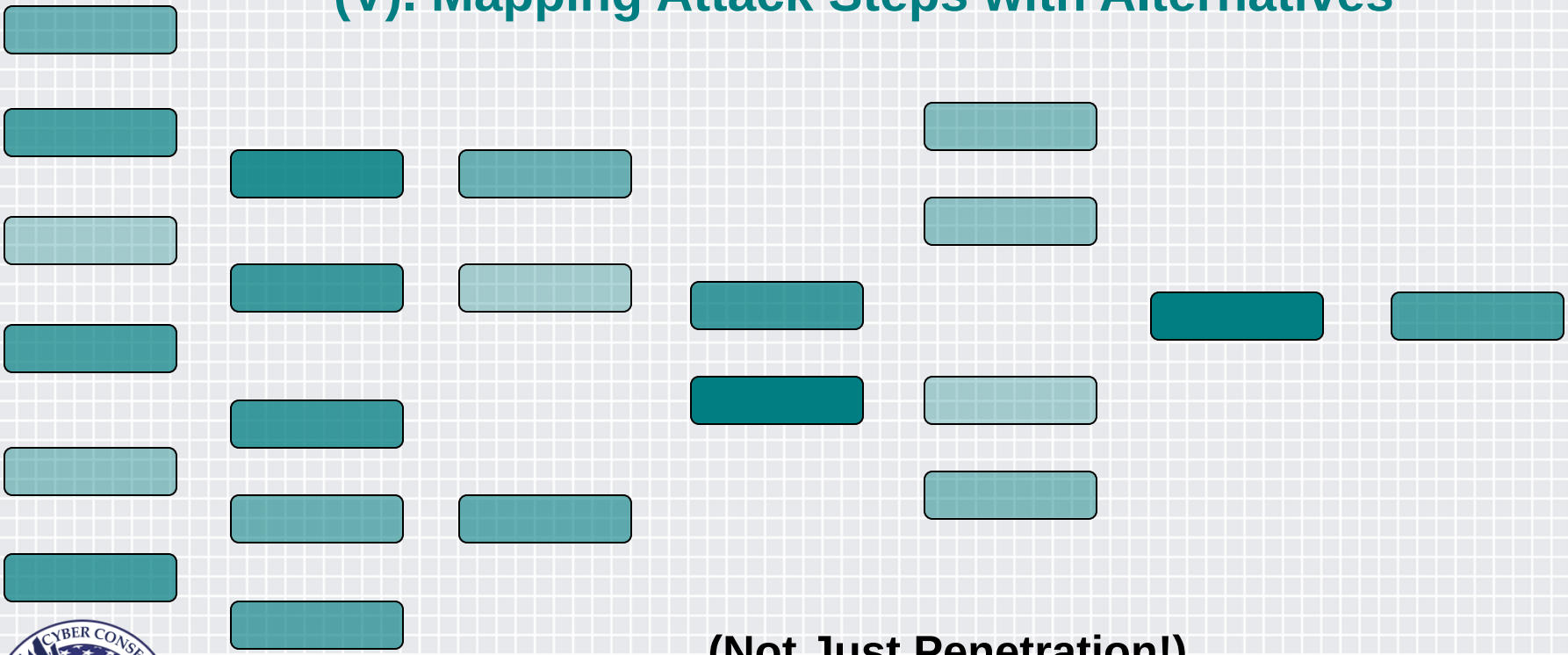
- If you can make the costs greater than the gains, you have won absolutely
- If you can make the costs significantly greater than other targets presenting similar gains, you have won relatively
- No attacker — not even a nation state — has unlimited resources

(V). Estimating Attacker Costs

Start with cost in time & expertise, not dollars:

- Lay out the attack steps (not just penetration) in a flow chart, including alternative paths
- Lay out the defenses on this flow chart
- Lay out the easily available attack tools for overcoming these defenses
- For each step, estimate the expertise level and the time required to use the easily available attack tools to overcome the defenses

(V). Mapping Attack Steps with Alternatives



(Not Just Penetration!)

EXPERTISE RATINGS FOR CYBER ATTACKS (BORG SCALE)	Comparative Score
Level Seven Expertise Nearly unique intellectual gifts or knowledge of highly secret systems	1,000,000's
Level Six Expertise Deep insider experience or very elite, specialized training	100,000's
Level Five Expertise Industry experience after a mid-level degree	10,000's
Level Four Expertise Solid mid-level university degree in the relevant subject	1000's
Level Three Expertise Relevant undergraduate coursework	100's
Level Two Expertise Sustained interest in a relevant discipline	10's
Level One Expertise A few days of web surfing by an intelligent student	1's
Level Zero Expertise No special skill or knowledge whatsoever	0

(V). Essential Types of Expertise in Identifying Costs

I. Business Expertise

(to chose the specific targets and types of attacks that would maximize benefits)

II. Access Expertise

(to devise ways of getting into the relevant information systems and to do so)

III. Process Expertise

(to know what exact information inputs or disruptions would produce the desired results)

IV. Programming Expertise

(to write the code and data entries that would produce the desired effects)

(V). Where Metrics from Actual Tests Can Be Useful

- Penetration tests
- Automated vulnerability scans
- Employee tests & exercises
- Work factor measurements for things like encryption

But only if these are reported in terms of the level of expertise and the time required from the attackers!

(V). Advantages of an Attacker Cost Metric

- The immediate (marginal) attacker cost can be estimated based on the vulnerabilities alone
- Once you know what and where the attacker costs are, you can figure out how and where you can most easily increase them
- Generally encourages risk-reducing actions

(V). Disadvantages of an Attacker Cost Metric

- Not a risk metric!
- Doesn't tell you whether or how much any given security measure is reducing your actual risk
- Wastes money by encouraging efforts to increase attacker costs where there would be hardly any attacker gains

Hence, while an Attacker Cost Metric is a good place to start, it is very important to move toward a genuine Risk Reduction Metric

Summary: What to Do

I. Don’t be distracted by dreams or promises of Fantasy Metrics!

II. Recognize Act-of-Desperation Survey Metrics for what they are!

III. Use Work Progress Metrics for measuring work progress and nothing else!

(Don’t be lulled by Maturity Level rationalizations!)

IV. Start working toward a genuine Three-Factor Risk Metric!

(Remember that rough numbers are better than no numbers!)

V. In the meantime, use an Attacker Cost Metric!

RSAConference2015

San Francisco | April 20-24 | Moscone Center

"You can't always get what you want. But if you try sometimes you just might find . . .You get what you need."

For advice or courses on how to generate & apply a real, three-factor risk metric, see www.usccu.us or contact scott.borg@usccu.us