
NORWICH
UNIVERSITY


Rational Risk Management: Balancing Costs and Benefits of Security Measures

Cybersecurity Conference

26 July 2006 – 13:00-16:00

M. E. Kabay, PhD, CISSP-ISSMP
Assoc. Prof. Information Assurance
Division of Business & Management, Norwich University
Program Director, MSIA
School of Graduate Studies, Norwich University
<mailto:mkabay@norwich.edu> V: 802.479.7937

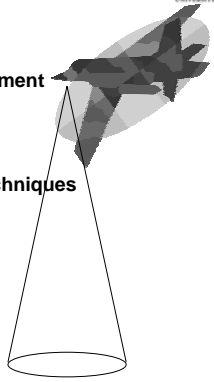
1 Copyright © 2006 M. E. Kabay. All rights reserved.


NORWICH
UNIVERSITY


Topics

- Part 1: Risk Assessment *
 - Definitions
 - Objectives of Risk Assessment
 - Limits of Questionnaires
 - A Model of Risk
 - Risk Mitigation
- Part 2: Risk Assessment Techniques
 - Questionnaires
 - Focus Groups
 - Interviews
 - Analytical Tools

* Based in part on Robert Jacobson's chapter in CSH4 (Bosworth & Kabay's Computer Security Handbook, 4th edition – Wiley, 2002)

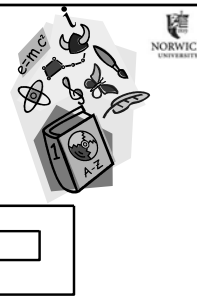


2 Copyright © 2006 M. E. Kabay. All rights reserved.


NORWICH
UNIVERSITY


Definitions

- Risk: *possibility of suffering harm or loss*
- Risk Management
 - Risk assessment
 - Risk mitigation
 - Security management
 - Security auditing
- Feedback ensures corrective actions back into process – continuous process improvement
- *Security is a process, not a state.*



3 Copyright © 2006 M. E. Kabay. All rights reserved.

Objectives of Risk Assessment




- Help to select subset of security measures given limitations on resources
- Every system will have unique security requirements
- Risk assessment must provide appropriate information about
 - ❑ Possible losses (costs of damage and of recovery)
 - ❑ Estimated probability of specific events or classes of events

4

Copyright © 2008 M. E. Kabay. All rights reserved.

A Model of Risk

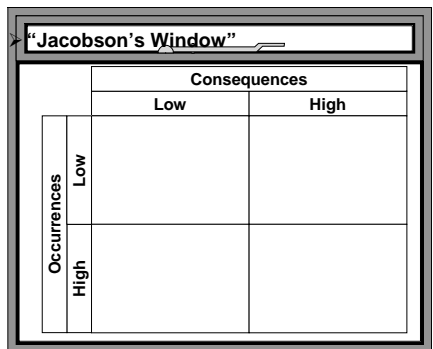
- Fundamental Risk Model
- Two Inconsequential Risk Classes
- Two Significant Risk Classes
- Real-World Risks & the ALE



5

Copyright © 2008 M. E. Kabay. All rights reserved.


Fundamental Risk Model



6

Copyright © 2008 M. E. Kabay. All rights reserved.

Two Inconsequential Risk Classes




		Consequences	
		Low	High
Occurrences	Low	Don't care	
	High		Doesn't happen

7

Copyright © 2006 M. E. Kabay. All rights reserved.

Two Significant Risk Classes




		Consequences	
		Low	High
Occurrences	Low		Major fire, long power outage, flooding, cash fraud,
	High	Power transient, minor sw bug, keystroke error,	

8

Copyright © 2006 M. E. Kabay. All rights reserved.

Real-World Risks & the ALE




➤ To compare risks, we use the *annualized loss expectancy* (ALE):

$$E(x) = \sum_i^{\infty} p_i c_i$$


➤ Where

- $E(x)$ = ALE of strategy x
- p_i = probability of occurrence i
- c_i = cost of occurrence i
- Σ = add up the products




9

Copyright © 2006 M. E. Kabay. All rights reserved.


Example of ALE Calculation 

Keystroke errors (Jacobson's example with slight modifications)

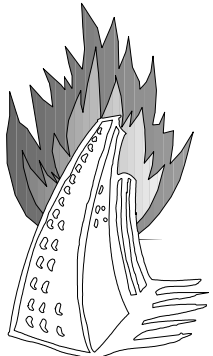
- 100 errors per operator per hour
- 100 operators
- 2,000 hours per operator per year
- = 20,000,000 errors per year
- Detection rate 99.9% at no cost
- Thus $p = 0.001$ failure rate of missed errors
- Errors corrected later @ \$1 each
- So $E(X) = 0.001 * 20,000,000 * \$1 = \$20,000$




10 Copyright © 2008 M. E. Kabay. All rights reserved.

Another ALE Calculation 

- Major fire (also Jacobson's example)
- Probability "p" of major fire in a year = 0.0001
- Cost of major fire estimated at \$100M
- Therefore $E(x) = 0.0001 \times \$100M = 10^{-4} \times \$10^8 = \$10^4 = \$10,000$



11 Copyright © 2008 M. E. Kabay. All rights reserved.

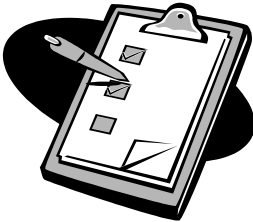
ALE of an Insurance Policy 

- Customer bets insurance company he will die this year (probability 0.1%)
- Bets (pays) \$750 in "premium"
- If customer dies, insurance company pays \$500,000 to widow
- Insurance company bets that customer lives – keeps premium, pays nothing.
 - $p_1 = 0.001$ $c_1 = -\$500,000$ (a gain to widow and a loss to the insurance company)
 - $p_2 = 0.999$ $c_2 = +\$750$ (a loss to family and a gain to the insurance company)
- $E(x) = \sum p_i c_i = 0.001 \times -\$500,000 + 0.999 \times +\$750 = +\$249.25$
(a loss to the family and a gain to the company)

12 Copyright © 2008 M. E. Kabay. All rights reserved.

Risk Mitigation


- Difficulties Applying ALE Estimates
- Risk Managers' Goals
- Mitigating Infrequent Risks
- Summary of Risk-Mitigation Strategies



13 Copyright © 2006 M. E. Kabay. All rights reserved.

Difficulties Applying ALE Estimates

- Information about information assurance risks is very poor
 - ❑ Little or no mandatory reporting
 - ❑ No centralized databanks
 - ❑ Therefore no actuarial statistics
- Jacobson's 30-Year Law
 - ❑ People dismiss risks not personally experienced in last 30 years
- Kabay's Paradox of Security
 - ❑ The better the security, the less direct evidence there is to support security measures

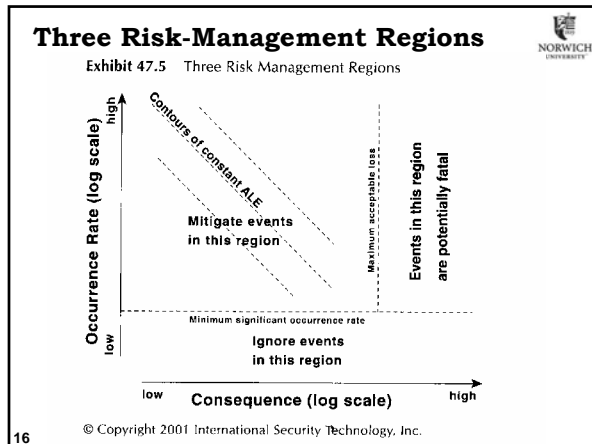


14 Copyright © 2006 M. E. Kabay. All rights reserved.

Risk Managers' Goals

- Imagine wide range of risks
- Try to estimate consequences / costs
- Attempt to determine probabilities
- Identify risk-mitigation strategies and their costs
- Compute ALEs to estimate appropriate return on investment (ROI)
 - ❑ Generally focus on loss-avoidance
 - ❑ However, some loss-avoidance can reduce costs to such a point as to provide overall increase in profitability
 - ❑ Also consider secondary effects such as improved customer relations, marketability, visibility in competitive marketplace....

15 Copyright © 2006 M. E. Kabay. All rights reserved.



Where ROI-Based Risk Mitigation is Effective

- Works well for high-probability, low-cost risk exposures
 - Realistic appraisal by managers
 - Data are credible
- Does not work well for low-probability, high-cost risk exposures
 - Upper management rarely understand implications of information technology risks
 - "Who would have thought...." common reaction by upper management

17 Copyright © 2008 M. E. Kabay. All rights reserved.

Four Reasons for Adopting a Mitigation Strategy

1. Required by law or regulations
2. Cost trivial but significantly lowers probability
3. Addresses low-probability, high-cost event with unacceptable SOL (single-occurrence loss); e.g., consequence that wipes out organization
4. Cost of mitigation is more than offset by expected reduction in ALE (i.e., positive ROI overall compared with doing nothing)

18 Copyright © 2008 M. E. Kabay. All rights reserved.

Mitigating Infrequent Risks

- Reduce magnitude of high SOLs*
 - ❑ Transfer risks using insurance
 - ❑ Disperse risk exposure (e.g., multiple ops centers)
 - ❑ Reduce vulnerability (e.g., BCP)
- Mitigation selection process
 - ❑ Choose low-cost measures
 - ❑ Ignore low risks
 - ❑ Use insurance to spread cash flow over years

* Single-occurrence losses

19

Summary of Risk-Mitigation Strategies (1)

Exhibit 47.6 A Quantitative Risk Mitigation Model


The graph plots Frequency of Occurrence (y-axis, low to high) against Consequence of Occurrence (x-axis, low to high). Three downward-sloping curves represent different risk strategies: 'Accept Risks' (leftmost), 'Mitigate Risks' (middle), and 'Transfer Risks' (rightmost). A vertical dashed line indicates the 'Max. tolerable SOL'. The area to the left of this line is labeled 'Doesn't Happen', and the area to the right is labeled 'Transfer Risks'. The text 'Don't Care' is located at the bottom left of the graph.

20

Summary of Risk-Mitigation Strategies (2)


- IT staff may be unable to reduce ALE of high-probability/low-consequence risks
- Midrange risks can be handled using mitigation measures chosen by evaluating their ROI using ALE calculations
- Low-probability/high-cost risks involve evaluations of SOLs and mitigation measures to reduce probabilities further or reduce costs through planning and preparation
- Ideally, risk management should be
 - ❑ Performed by experts
 - ❑ Independent of IT management
 - ❑ Reported to senior management directly

21

Risk Assessment Techniques 

- Aggregating Threats and Loss Potentials
- Basic Risk-Assessment Algorithms
- Loss-Potential
- Risk Event Parameters
- Vulnerability Factors, ALE, SOL Estimates
- Sensitivity Testing
- Selecting Risk-Mitigation Measures


22 Copyright © 2008 M. E. Kabay. All rights reserved.

Aggregating Threats and Loss Potentials 

- Calculations of ALE can be increased in precision using aggregation of individual ALEs for specific components of systems
 - E.g., if manufacturers provide failure rates for specific components (e.g., servers), these data can be helpful in estimating overall failure rates
- One useful rule: probability P of failure of a system with independent units "i" where each has probability p_i of failing is

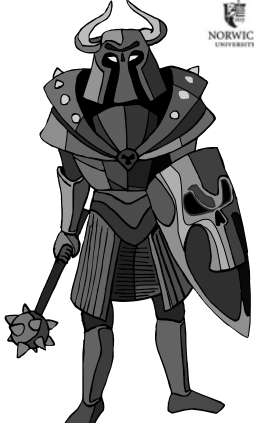
$P = 1 - \prod(1-p_i)$ which reduces to $P = 1 - (1-p)^n$ for systems where all the units have the same p_i

23 Copyright © 2008 M. E. Kabay. All rights reserved.


Loss-Potential 

Loss potential can include costs of

- Property damage
- Liability
- Service interruption




24 Copyright © 2008 M. E. Kabay. All rights reserved.

Risk Event Parameters 


- Occurrence rate estimation
 - ❑ Rates often change after problems occur
 - ❑ Don't count events twice; e.g., if a power failure causes a system crash, be careful not to count both of these separately
 - ❑ Look for external source of actuarial data
- Outage duration affects costs
 - ❑ Service interruption increasingly important with e-commerce growing
 - ❑ EDI, Web purchases, multiple competitors....

25 Copyright © 2006 M. E. Kabay. All rights reserved.

Vulnerability Factors, ALE, SOL Estimates 

- Validating the estimates is important
- Check all the individual data and calculations before basing decisions on math
- Look for the risk event/loss potential pairs that generate ~80% of total ALE
- Check assumptions – discuss with team members
- Look for outliers – extraordinarily large contributors – and double-check them

26 Copyright © 2006 M. E. Kabay. All rights reserved.

Sensitivity Testing 

- Estimates of probability and costs are unlikely to be point-estimates
- Can use range estimates
 - ❑ Try high, medium and low
- If probability distributions are available, try Monte Carlo simulation
 - ❑ Run random trials selecting values from parameter distributions
 - ❑ Plot range of resulting ALEs to see central tendencies
 - ❑ Look out for chaotic systems

27 Copyright © 2006 M. E. Kabay. All rights reserved.

Selecting Risk-Mitigation Measures

- Address intolerable SOLs
- Discard mitigation with negative ROIs (but remember that insurance always has a short-term negative ROI)
- Rank measures by descending benefits, costs, ROI

28 Copyright © 2008 M. E. Kabay. All rights reserved.




BREAK 17'13"

29 Copyright © 2008 M. E. Kabay. All rights reserved.




Methods for Qualitative Risk Assessment and Prioritization

- Questionnaires
- Focus groups
- Interviews
- Delphi Technique
- Computer-Aided Consensus




30 Copyright © 2008 M. E. Kabay. All rights reserved.



Limits of Questionnaires 


- Could a security questionnaire suffice as a risk assessment?
 - Ask people for their opinions
 - Collate the results
- Problems
 - Ambiguities in use of words (“serious”, “expensive”....
 - Many questions prompt yes/no answers but need more subtle distinctions
 - Questionnaires miss points that arise in open discussion with back-and-forth exchange of ideas

31 Copyright © 2008 M. E. Kabay. All rights reserved.

Designing Effective Questionnaires (1) 

- People unconsciously try to please others
 - May give what they think/feel is *expected* answer
 - Tend to answer “Yes” to whatever is asked
- Therefore avoid leading questions
 - “Do you think that the most important issue in our security plans is employees?”
 - Try “What is the most important issue in our security plans?”

32 Copyright © 2008 M. E. Kabay. All rights reserved.

Designing Effective Questionnaires (2) 

- Some respondents will automatically check all the high or low answers
 - Avoid having all scales in the questions pointing same way (1 low – 5 high)
- Some respondents will lie
 - Introduce internal validation
 - Ask same question in two different ways in different parts of the questionnaire
 - ✓ Q14 “Which of the following is the lowest risk?”
 - ✓ Q72 “Which of the following is the highest risk?”

33 Copyright © 2008 M. E. Kabay. All rights reserved.

Designing Effective Questionnaires (3)



- Sometimes questions influence answers to neighboring questions
 - ❑ E.g., giving a high estimate in Q22 may lead to a higher answer in Q23
 - ❑ Therefore prepare different versions of the questionnaire which have different question sequences
- Be careful about closed vs open questions
 - ❑ Pre-determined scales may influence answers (e.g., "Estimate the total cost / \$1K, \$10K, \$100K, \$1M, \$10M" will skew results)
 - ❑ Can simply ask "Estimate the total cost" and let respondent choose range of answer

34

Copyright © 2008 M. E. Kabay. All rights reserved.

Focus Groups



- Small group of people brought together to discuss thoughts, feelings, analyses of specific problem
- Can be highly productive
- Normally recorded and analyzed in detail later
- Important to keep atmosphere positive and open to all ideas
- Can also use brainstorming techniques



35

Copyright © 2008 M. E. Kabay. All rights reserved.

Brainstorming



- Goal: generate ideas to solve problem
- Separate ideation from analysis
 - ❑ 2 phases: find/create ideas then organize
- Ideation
 - ❑ Set numerical goal (e.g., "100 ideas on how to...")
 - ❑ No critical (negative or positive) responses
 - ❑ Write every idea down on large paper
 - ✓ Including silly ones
 - ✓ Post sheets on walls
- 100, now let's find 10 more!"




36

Copyright © 2008 M. E. Kabay. All rights reserved.

Brainstorming (cont'd)


- Facilitator encourages ideation
- Scribe writes everything down
 - ❑ Also ideal to record discussions
- Participants
 - ❑ Should have means for making notes – avoid losing new ideas
 - ❑ Should not go into any detail
 - ❑ Cryptic suggestions are *good*
- Hitchhiking
 - ❑ When an idea sparks a new one, use hand signal to indicate priority (to avoid forgetting)



Copyright © 2006 M. E. Kabay. All rights reserved.

Interviews

- One-on-one discussions with appropriate people
 - ❑ “I need your help. Can you work with me to identify key areas where we need to improve security from your perspective?”
- Individuals know their own work better than anyone else
 - ❑ Can lead to deep insights into process
 - ❑ Often have unspoken ideas on problems and possible solutions



Copyright © 2006 M. E. Kabay. All rights reserved.

Analyzing Results from Focus Groups & Interviews

- Sometimes have enormous mass of material
- May not know where to start in making sense of findings
- Offer proposals to panel of experts and ask them to use *Delphi Technique* to come to consensus
- Can also refine brainstorming using *Computer-Aided Consensus™ (CAC)*
- Can use *Computer-Aided Thematic Analysis™ (CATA)* to sort through masses of ideas

Copyright © 2006 M. E. Kabay. All rights reserved.

Delphi Technique

- RAND Corporation, 2nd World War
- Develop quantitative estimates using expert opinion
- Ask top and bottom quartiles to *explain reasons*
- Share reasons
- Estimate again
- Iterate to stability

40 Copyright © 2008 M. E. Kabay. All rights reserved.

Computer-Aided Consensus

- Real-time Delphi Technique
- Need a spreadsheet & printer or network
- 1st, determine operational scale of importance
 - How much time?
 - How much money?
 - When to start?
- Agree on simple scale; e.g.,

<input type="checkbox"/> 1 = start this week	OR	spend \$0
<input type="checkbox"/> 2 = this month		\$1,000
<input type="checkbox"/> 3 = this quarter		\$10,000
<input type="checkbox"/> 4 = this year		\$100,000
<input type="checkbox"/> 5 = never		\$1,000,000


41 Copyright © 2008 M. E. Kabay. All rights reserved.

Computer-Aided Consensus (cont'd)

- Lay out results of brainstorming or other list
 - Use spreadsheet
 - 1 idea/proposal per row
- Define 1 column per participant
- Enter each participant's estimate of importance / priority / value in column beside ideas / proposals
- Can collect scores using printouts or using networked computers to fill in spreadsheets

Idea	Bob	Jane	Karim	Robbie
Javelin	2	4	3	1
Halberd	3	3	3	1
Morningstar	2	5	3	4
Broadsword	5	2	3	2
Pike	1	3	2	5
Ballista	2	2	2	2
Retarius	1	5	3	4
Bombard	4	3	3	3


42 Copyright © 2008 M. E. Kabay. All rights reserved.

Computer-Aided Consensus (cont'd) 

- Calculate average and variance
- Sort descending by priority / importance

Idea	Bob	Jane	Karim	Robbie	avg	var
Morningstar	2	5	3	4	3.5	1.7
Halberd	3	6	4	1	3.3	2.9
Broadsword	5	3	4	3	3.0	2.0
Ballista	2	2	2	2	3.0	0.7
Pike	1	5	3	5	2.8	2.9
Bombard	4	1	2	1	2.0	2.0
Retarius	1	3	2	2	2.0	0.7
Javelin	2	1	1	1	1.3	0.3

43 Copyright © 2006 M. E. Kabay. All rights reserved.


Computer-Aided Consensus (cont'd) 

- Group *roughly* by class of priority / importance
- Sort downward by *variance* within subgroup
- Discuss *reasons* for greatest variation in estimated priority / importance among *most important proposals / ideas*

Idea	Bob	Jane	Karim	Robbie	avg	var
Halberd	3	6	4	1	3.3	2.9
Broadsword	5	3	4	3	3.0	2.0
Morningstar	2	5	3	4	3.5	1.7
Ballista	2	2	2	2	3.0	0.7
Pike	1	5	3	5	2.8	2.9
Bombard	4	1	2	1	2.0	2.0
Retarius	1	3	2	2	2.0	0.7
Javelin	2	1	1	1	1.3	0.3

Why so much disagreement?
Arbitrarily defined top (most important) group

44 Copyright © 2006 M. E. Kabay. All rights reserved.

Computer-Aided Consensus (cont'd) 

- Spend *most time* on *important* issues where people *disagree*
- Discussing differences reveals new information about why people diverge:
 - different assumptions
 - divergent priorities
 - unshared or contradictory information
 - different reasoning
 - errors
- Sharing info and resolving differences on important issues speeds consensus

45 Copyright © 2006 M. E. Kabay. All rights reserved.

Computer-Aided Consensus (cont'd)



- Extremely important not to generate hostility
- Best if spreadsheet visible for everyone
 - ❑ Projector
 - ❑ Network with net-meeting software
- Keep track of explanations for divergences
 - ❑ Use brainstorming techniques
- Make process as dynamic as you can
 - ❑ Change priorities in spreadsheet as often as needed
 - ❑ Recalculate and sort again

46

Copyright © 2006 M. E. Kabay. All rights reserved.

Computer-Aided Thematic Analysis (CATA)



- How can we *organize non-quantitative knowledge without imposing extrinsic framework*
- Extrinsic frameworks (preconceived notions)
 - ❑ Can interfere with development of novel insight
 - ❑ May mask data that don't fit preconceptions
- Intrinsic frameworks
 - ❑ Develop by examination of data themselves
 - ❑ Work with existing frameworks but go beyond conventional ideas

47

Copyright © 2006 M. E. Kabay. All rights reserved.

Overview of CATA




- Define themes
- Write one theme per line in spreadsheet
- Keep track of origin
- Develop intrinsic framework for classification
- Apply preliminary classification
- Sort
- Classify again using finer granularity
- Repeat sort/classify until stable
- Report using synthetic paragraphs

48

Copyright © 2006 M. E. Kabay. All rights reserved.

Define Themes



- “Theme”
 - ❑ Any expression of fact, opinion or feeling
 - ❑ “This project started 18 months ago.”
 - ❑ “This project has been running too long.”
 - ❑ “I hate this project.”
- Break down all sentences
 - ❑ at punctuation marks (. , ; : ! ?)
 - ❑ at some conjunctions (and, but)
- Insert hard-return (line-break) to demarcate themes
 - ❑ Use global find-replace function

49 Copyright © 2006 M. E. Kabay. All rights reserved.

Enter Themes into Spreadsheet

- Paste (copy) text into spreadsheet
 - ❑ One theme per line in spreadsheet
- Keep track of origin
 - ❑ 1 column per source / person

1	Theme	Source					
		RB	UR	BT	AJ	Text 1	Paper 1
2		*					
3	Managers don't listen to us;	*					
4	they ask us for our opinion	*					
5	but they ignore them when they write up the reports.	*					
6	Our managers really listen to us;		*				
7	they ask us for our opinion		*				
8	and incorporate what we say into their recommendations.		*				
9	Everyone seems really concerned about security.			*			
10	Security is a joke in this organization.			*			
11	The president wears an ID badge to set a good example			*			
12	Our security awareness program keeps us up to date,				*		
13	I enjoy the case histories they put in the company newsletter.				*		
14	Walking what you talk is an essential part of establishing good security.					239	

51 Copyright © 2006 M. E. Kabay. All rights reserved.

Develop Intrinsic Framework for Classification

- Read through the (huge) list of themes
- Jot down any word that
 - ❑ Occurs spontaneously to you
 - ❑ Could help you organize themes
- Look through categories or *metathemes*
 - ❑ Organize, order, number metathemes
 - ❑ Stick to 6-10 metathemes if possible
 - ❑ E.g.,
 - 1 Current status
 - 2 Policy development
 - 3 Awareness program
 - 4 Psychological issues

51 Copyright © 2006 M. E. Kabay. All rights reserved.

Apply Preliminary Classification & Sort

- Insert 2 columns to left of themes
- Generate sequence number for each line
 - To keep connected themes together
- Classify each theme by noting number (or letter) of the appropriate metatheme
- Sort entire list (including origin columns) by
 - Metatheme; and
 - By sequence number within metatheme
- See next slides for illustrations

	A	B	
1	Seq #	Metatheme	Theme
2			
3	1	1	
4	2	2	
5	3	2	
6	4	4	

52 Copyright © 2006 M. E. Kabay. All rights reserved.

Preliminary Classification

	A	B	C				D	E	F	G	H	I
1	Seq #	Metatheme	Theme				Source					
2							RB	UR	BT	AJ	Text 1	Paper 1
3	1	1					*					
4	2	2					*					
5	3	2					*					
6	4	4						*				
7	5	3						*				
8	6	3						*				
9	7	4						*				
10	8	2							*			
11	9	3							*			
12	10	1							*			
13	11	4							*			
14	12	2								239		
15	13	3										4

53 Copyright © 2006 M. E. Kabay. All rights reserved.

Sort

- By metatheme
- And by sequence number

Seq #	Metatheme	Theme	RB	UR	BT	AJ	Text 1	Paper 1
1	1							
10	1							
3	2							
8	2							
12	2							239
2	3							
5	3							
6	3							
9	3							
13	3							
4	4							4
7	4							
11	4							

Sort

Sort by: **Metatheme** Ascending Descending


Then by: **Seq #** Ascending Descending

My list has: Header row No header row

Options... OK Cancel

54

Classify Again Using Finer Granularity & Sort




1	0	Current status
2	0	Policy development
3	0	Awareness program
4	0	Psychological issues
1	1	Beliefs
1	2	Attitudes
1	3	Behavior
2	1	Working group
2	2	Mission
2	3	Style
3	1	Contract
3	2	Performance
3	3	Newsletter
3	4	Courses
3	5	Games
3	6	Contests
3	7	Posters
3	8	Rewards
4	1	Role models
4	2	Entitlement
4	3	Alienation

- Examine each group of items under one metatheme
- As required, subdivide metathemes
 - ☐ Grouping helps identify subdivisions
 - ☐ Original metathemes become “n – 0”
- Introduce another column into listing
- Rate each theme according to two-part metathemes
- Duplicate lines for more than 1 metatheme
- Reorganize metathemes as needed
 - ☐ Can use find-replace function and sort to move whole blocks

Copyright © 2006 M. E. Kabay. All rights reserved.

Report Using Synthetic Paragraphs



- When satisfied at organization of data, can start writing report
- “-0” items serve as headings and sub-headings
- Summarize findings and combine quotations that are in the same direction as one synthetic paragraph; e.g.,

“Most employees felt that management were listening to their feelings:
Managers really listen to us. They pay attention to our suggestions.”

56

Copyright © 2006 M. E. Kabay. All rights reserved.

DISCUSSION



57

Copyright © 2006 M. E. Kabay. All rights reserved.
