

# Role(s) of the CISO

CSH5 Chapter 65  
“ROLE OF THE CISO”  
Karen Worstell

1

Copyright© 2014 M. E. Kabay. All rights reserved.

## Topics

- CISO AS CHANGE AGENT
- CISO AS STRATEGIST
- STRATEGY, GOVERNANCE, AND THE STANDARD OF CARE
- RECOMMENDATIONS FOR SUCCESS FOR CISOs



Karen F. Worstell

2

Copyright© 2014 M. E. Kabay. All rights reserved.

## CISO AS CHANGE AGENT

- CIO responsibilities broad
  - ❑ CISO role broadening beyond IT security
  - ❑ CISO focuses on information security
- CISO manages trust
  - ❑ People, business processes, technology
  - ❑ Enterprise & its partners – stakeholders
  - ❑ Must coordinate with CIO & CSO (Chief Security Officer)
- Technology has spawned new attack vectors
- Legislation
  - ❑ Increasingly forcing responsibility and disclosure for consumer/data subjects
  - ❑ Increasing penalties for failure
  - ❑ Preparing / defending against litigation growing in importance
- CISO must clarify obligations, necessities & strategic spending

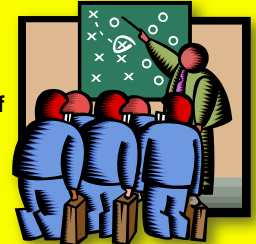


3

Copyright© 2014 M. E. Kabay. All rights reserved.

## CISO AS STRATEGIST

- Overview: Strategic Situational Awareness
- Reliance on Digital Information
- Inherent Insecurity of Systems
- World Trends



4

Copyright© 2014 M. E. Kabay. All rights reserved.

## Overview: Strategic Situational Awareness (1)

- Information growing in value
  - ❑ “Information is the business.”\*\*
  - ❑ Information applications determine competitive advantage
  - ❑ Require rules-based protection to ensure data control, confidentiality, integrity, authenticity, availability & utility



\* Phil Condit, former chairman of Boeing, speaking at Intl Info Integrity Inst (I4) in 1995

5

Copyright© 2014 M. E. Kabay. All rights reserved.

## Overview: Strategic Situational Awareness (2)

- Main drivers for CISOs to define new strategy for information security
  - ❑ Systems inherently insecure
    - ✓ Variations in configuration
    - ✓ Complexity
    - ✓ Volume of vulnerabilities
  - ❑ Reach of global business increases complexity
    - ✓ Business processes
    - ✓ Personnel
    - ✓ Business systems
  - ❑ Asymmetrical warfare
    - ✓ Vastly more attackers than defenders in an organization
    - ✓ Attack vectors change quickly
    - ✓ Trusted insiders are most significant threat




6

Copyright© 2014 M. E. Kabay. All rights reserved.

### Overview: Strategic Situational Awareness (3)

- CISO as strategist must
  - ❑ Adopt & integrate new methods
  - ❑ Update current methods of protection
    - ✓ Network defenses
    - ✓ Data classification
- CISO must adopt long-term business strategic thinking
  - ❑ Consider reliance on information
  - ❑ Define & explain why protection is important
  - ❑ Cope with fundamentally insecure systems
  - ❑ Abandon risk-based security thinking



7

Copyright© 2014 M. E. Kabay. All rights reserved.

### Reliance on Digital Information

- 85% of US critical infrastructure owned by private companies
- Interconnecting systems force a chain of trust
  - ❑ Trust in systems to trust in information
  - ❑ Trust in information to trust in decisions
- May be forced to demonstrate
  - ❑ Digital ownership of intellectual property (IP)
  - ❑ Chain of possession of IP

#### CRITICAL INFRASTRUCTURE


1. Information technology
2. Telecommunications
3. Chemicals
4. Transportation systems
5. Emergency systems
6. Postal & shipping services
7. Agriculture & food
8. Public health & healthcare
9. Drinking water / water treatment
10. Energy
11. Banking & finance
12. National monuments & icons
13. Defense industrial base
14. Key industry/technology sites
15. Large gathering sites

8

Copyright© 2014 M. E. Kabay. All rights reserved.

### Inherent Insecurity of Systems

- Components of systems all created / installed by (fallible/corruptible) human beings
  - ❑ Hardware, software
  - ❑ Utilities, scripts
  - ❑ Transport media
- All irretrievably flawed
  - ❑ Vulnerabilities (current & future) cannot all be addressed / redressed
  - ❑ Perfect security is myth: unattainable
  - ❑ Risk-based methods don't work
    - ✓ Unscaleable
    - ✓ No meaningful data for probability
    - ✓ Annualized loss expectancies (ALE) impossible to verify




9

Copyright© 2014 M. E. Kabay. All rights reserved.

### World Trends (1)

- Dramatic geographic shifts in economic activity
  - ❑ Supply chains & internal processes will be globalized
  - ❑ Outsourcing, leasing will complicate asset protection
- Increased connectivity will disrupt current security infrastructures
  - ❑ Mobile devices will affect rules on inbound & outbound filters
  - ❑ Huge increase in data density of storage devices must alter security processes
  - ❑ Grid / cloud computing changes rules



10

Copyright© 2014 M. E. Kabay. All rights reserved.

### World Trends (2)

- New models for information processing require new rules or new models
  - ❑ Cloud computing
  - ❑ Software as a service (SaaS)
  - ❑ Access to proprietary information over the Web
    - ✓ E.g., telecommuting by employees
- CISO must function at level of executive management
  - ❑ Business strategist
  - ❑ Participate in executive leadership team
  - ❑ Enable integration of due diligence to standard of care into all business streams



11

Copyright© 2014 M. E. Kabay. All rights reserved.

### STRATEGY, GOVERNANCE, & THE STANDARD OF CARE

- Standard of Care
- Governance & Accountability
- Roles & Responsibilities
- Reporting
- Monitoring
- Metrics
- Executive Visibility




12

Copyright© 2014 M. E. Kabay. All rights reserved.

### Standard of Care (1)


- Key vision
  - ❑ Put in place mechanisms for
  - ❑ Enabling business to demonstrate
  - ❑ Due diligence
  - ❑ To appropriate standard of care
- Basic steps
  - ❑ Evaluate risk qualitatively
    - ✓ High – medium – low
    - ✓ NOT using quantitative methods such as ALE
  - ❑ Use accepted standards as framework
  - ❑ Translate high-level policy into action



13

### Standard of Care (2)

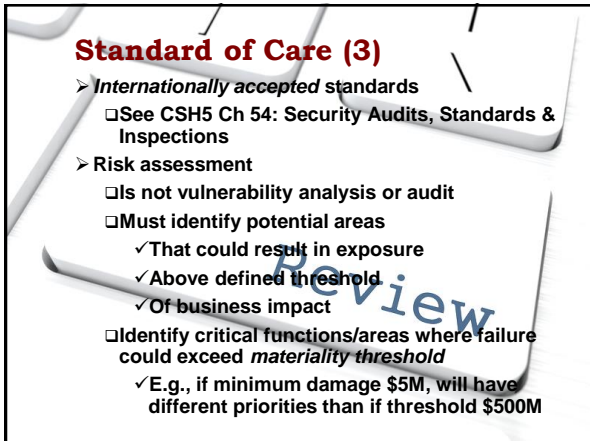
- Internationally accepted for standards of due care include
  - ❑ ISO/IEC 17799:2005
  - ❑ ISO/IEC 27001:2005
  - ❑ ISO/IEC 13335-1:2004
  - ❑ COBIT® – Control Objectives for IT
  - ❑ ITIL® – IT Infrastructure Library
- See Exhibit 65.1 & also CSH5 chapters
  - ❑ 44 “Security Policy Guidelines”
  - ❑ 54 “Security Audits, Standards, and Inspections”



14

### Standard of Care (3)


- Internationally accepted standards
  - ❑ See CSH5 Ch 54: Security Audits, Standards & Inspections
- Risk assessment
  - ❑ Is not vulnerability analysis or audit
  - ❑ Must identify potential areas
    - ✓ That could result in exposure
    - ✓ Above defined threshold
    - ✓ Of business impact
  - ❑ Identify critical functions/areas where failure could exceed *materiality threshold*
    - ✓ E.g., if minimum damage \$5M, will have different priorities than if threshold \$500M



15

### Standard of Care (4)

- CISO does not micromanage
- CISO assigns duties to appropriate staff
  - ❑ Detailed configuration of devices role of security officers & other employees
- CISO reviews reports
- CISO ensures continuous process improvement
- Bruce Schneier: “In the real world, security involves processes. It involves preventative technologies, but also detection and reaction processes, and an entire forensics system to hunt down and prosecute the guilty. Security is not a product; it itself is a process. And if we’re ever going to make our digital systems secure, we’re going to have to start building processes.”\*

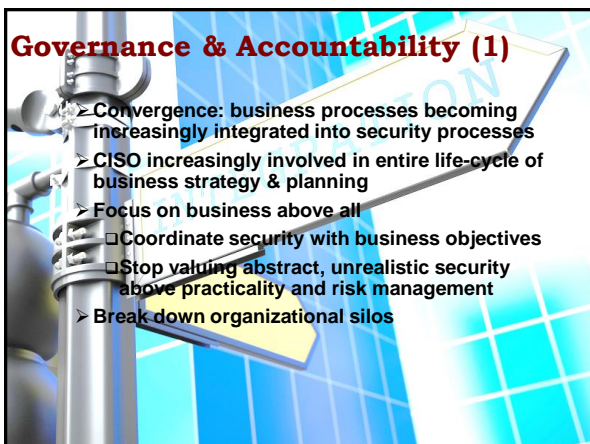


Preface to *Secrets and Lies* (2004).  
<http://www.schneier.com/book-sandl-pref.html>

16

### Governance & Accountability (1)

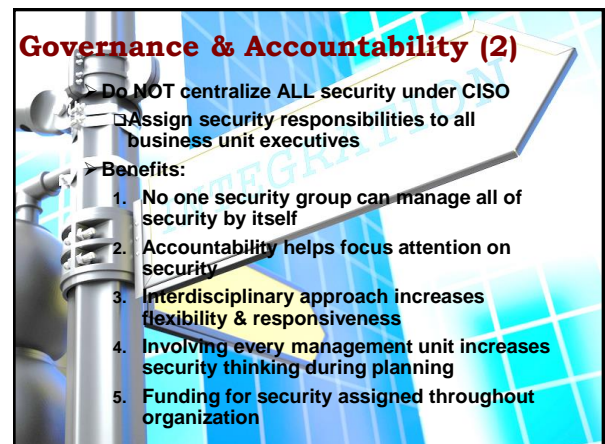
- Convergence: business processes becoming increasingly integrated into security processes
- CISO increasingly involved in entire life-cycle of business strategy & planning
- Focus on business above all
  - ❑ Coordinate security with business objectives
  - ❑ Stop valuing abstract, unrealistic security above practicality and risk management
- Break down organizational silos



17

### Governance & Accountability (2)

- Do NOT centralize ALL security under CISO
  - ❑ Assign security responsibilities to all business unit executives
- Benefits:
  1. No one security group can manage all of security by itself
  2. Accountability helps focus attention on security
  3. Interdisciplinary approach increases flexibility & responsiveness
  4. Involving every management unit increases security thinking during planning
  5. Funding for security assigned throughout organization




18

### Governance & Accountability (3)

Policy-driven approach to IA/BCP/DRP governance


<b>Senior Leadership Team (C-level)</b>	<ul style="list-style-type: none"> <li>Authority for policy</li> <li>Governance body</li> <li>Program oversight</li> </ul>
<b>Policy</b>	<ul style="list-style-type: none"> <li>Accountability</li> <li>Programs &amp; program authority</li> <li>Governance processes</li> <li>Publishes under authority of entire senior leadership team</li> </ul>
<b>Principles</b>	<ul style="list-style-type: none"> <li>5-6 high-level statements at descriptive level</li> <li>Separate from policy</li> <li>Establishes guidance for business unit standards</li> </ul>
<b>Business Unit Team</b>	<ul style="list-style-type: none"> <li>Staff support</li> <li>Facilitates governance process</li> <li>Provides technical leadership for security across business units</li> <li>Representatives from each business unit + audit</li> <li>CISO = chair</li> <li>Coordinates policy principles for senior leadership team approvals</li> <li>Standards at prescriptive level</li> <li>Implements standards</li> <li>Monitors effectiveness (metrics, reports)</li> <li>Coordinates continuous process improvement for security across all business units</li> </ul>



19

### Governance & Accountability (4)




- CISO must become agent of change
  - ❑ Move from implementation
  - ❑ Move to innovation & responsiveness to business needs
- Attack profiles changing
  - ❑ Moving away from simple technical exploits
  - ❑ Moving to targeted exploitation of business process weaknesses
  - ❑ Every executive must be thinking about security as normal part of business management



20

### Roles & Responsibilities (1)


- Convince upper management that CISO must be agent of change
  - ❑ Refer to best practices
    - ✓ Institute of Internal Auditors (IIA)
    - ✓ Information Security and Control Association (ISACA)
    - ✓ IT Governance Institute (ITGI)
  - ❑ Adapt to specific needs of organization
- Expect incremental change, not instant compliance
- Use 10 principles (next slides) as discussion points

21

### Roles & Responsibilities (2)

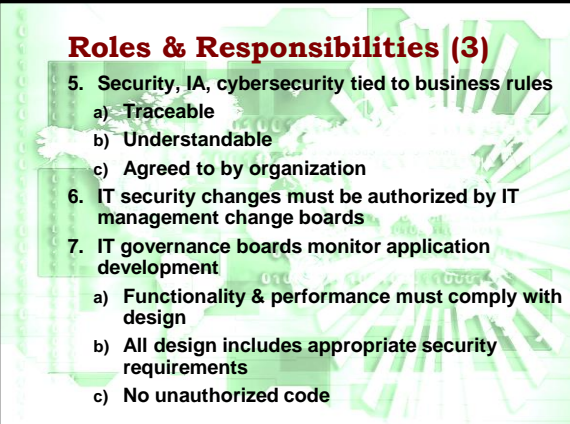
1. CISO doesn't own/control IT assets – manages them for effective business results
2. Independent auditor regularly reviews implementation
3. IT security expenses must be justified by business value
4. IT security monitored by IT governance board
  - a) IT
  - b) Business management
  - c) CFO



22

### Roles & Responsibilities (3)


5. Security, IA, cybersecurity tied to business rules
  - a) Traceable
  - b) Understandable
  - c) Agreed to by organization
6. IT security changes must be authorized by IT management change boards
7. IT governance boards monitor application development
  - a) Functionality & performance must comply with design
  - b) All design includes appropriate security requirements
  - c) No unauthorized code



23

### Roles & Responsibilities (4)

8. IT security operations & processes managed tightly: standardized, documented, reviewed regularly by IT management & independent auditors
  - a) New processes adapt to business change
  - b) Existing processes regularly reviewed, including involvement by legal counsel
9. Information systems assets have clear ownership / accountability
  - a) Assets used as intended
  - b) Assets accessed according to authorization
  - c) Assets available and useful according to metrics (e.g., QoS\*)



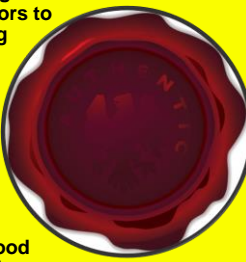
24

## Roles & Responsibilities (5)

10. Appropriate & updated training & certification of IT employees, contractors, vendors to ensure capability for enforcing security

➤ Final remarks:

- ❑ Major hurdle: business managers generally don't understand IT & would prefer to see it controlled by "IT staff"
- ❑ Must convince upper management that IT is lifeblood of business: no info, no business
- ❑ Accepting responsibility / accountability for all aspects of IT & security radically changes level of cooperation



25

Copyright © 2014 M. E. Kabay. All rights reserved.


## Reporting & Accountability

➤ Governance structure leads to appropriate assignment of accountability

- ❑ Not *if* but *how* managers take responsibility for results

➤ Without accountability

- ❑ Rules will not be implemented well
- ❑ Enforcement will fail



26

Copyright © 2014 M. E. Kabay. All rights reserved.

## Monitoring

➤ How well are we doing in meeting our standards?

- ❑ Kabay: REALITY TRUMPS THEORY


➤ Monitoring allows decisions for specific areas

- ❑ Controls are working
- ❑ Controls are not working

➤ Close coordination with internal audit

➤ Standards

- ❑ Objective standards of proof
- ❑ Hearsay inadequate
- ❑ Must expect to automate data gathering



27

Copyright © 2014 M. E. Kabay. All rights reserved.


## Metrics

➤ Choose metrics carefully: must be essential to

- ❑ Provide performance indicators
- ❑ Be actionable: actually provide options for making changes

➤ Monitoring what cannot be changed is pointless

- ❑ Attacks on perimeter meaningless unless we also measure attacks *penetrating* perimeter
- ❑ Thus have ID\* outside firewalls & inside firewalls



28

Copyright © 2014 M. E. Kabay. All rights reserved.

\*Intrusion Detection

## Executive Visibility


➤ CISO executive scorecard

- ❑ Published w/ support of C-level sponsor(s)
- ❑ Helps drive behavior according to metrics reported

➤ Quarterly reports (or more frequent)

➤ Support continuous process improvement

➤ Encourage executive / managerial involvement



**High visibility clothing must be worn**

29

Copyright © 2014 M. E. Kabay. All rights reserved.

## RECOMMENDATIONS FOR SUCCESS FOR CISOs

➤ Education & Experience

➤ Culture of Security in the Business

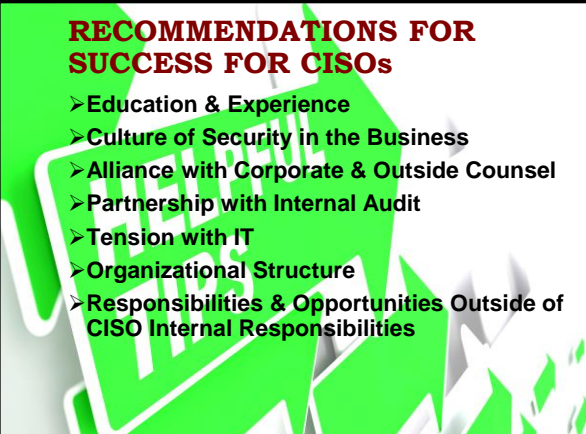
➤ Alliance with Corporate & Outside Counsel

➤ Partnership with Internal Audit

➤ Tension with IT

➤ Organizational Structure

➤ Responsibilities & Opportunities Outside of CISO Internal Responsibilities



## Education & Experience (1)

### Leadership skills

- Wise counsel / appropriate judgement
- Big picture view
- MBA degree may be helpful
- Life experience of value
- Studying reputable books on management & leadership helpful
- Keep up to date on IT & security developments



31

Copyright©2014 M. E. Kabay. All rights reserved.

## Education & Experience (2)

### Know your organization's functional organization

- Core stakeholders:
  - ❑ Internal audit
  - ❑ Legal counsel
  - ❑ Business executives
  - ❑ IT staff
- Frequent discussions with
  - ❑ Finance
  - ❑ Supply chain
  - ❑ Human resources



32

Copyright©2014 M. E. Kabay. All rights reserved.

## Education & Experience (3)

### Know your company's mission-critical objectives & processes

- Company's value chain\*
- Major business processes
- Disclosure statements
- Annual reports
- Major cost concerns
- Major revenue streams
- Key risks (outside security)



\*Value chain: sequence of activities at each of which products gain value.

Ref: Porter, M. (1985). *Competitive Advantage: Creating and Sustaining Superior Performance*. Free Press (ISBN 0-684-84146-0). 592 pp. Index.

33

Copyright©2014 M. E. Kabay. All rights reserved.

## Culture of Security in the Business (1)

- Study culture: attitudes toward
  - ❑ Accepting direction
  - ❑ Allowing time & resources to be used for security
- Questions for understanding organizational culture towards security
  1. Risk appetite: materiality threshold for risk management?
  2. Norms / attitudes:
    - ✓ High turnover, tolerance for change, focus on autonomy? Or
    - ✓ Policy-driven bureaucracy?
    - ✓ Generally use reward in preference to punishment

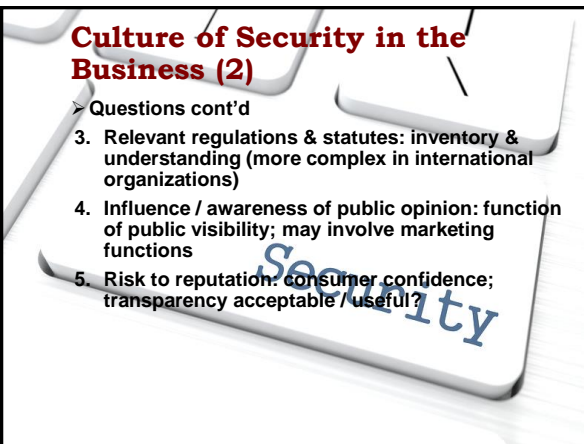


34

Copyright©2014 M. E. Kabay. All rights reserved.

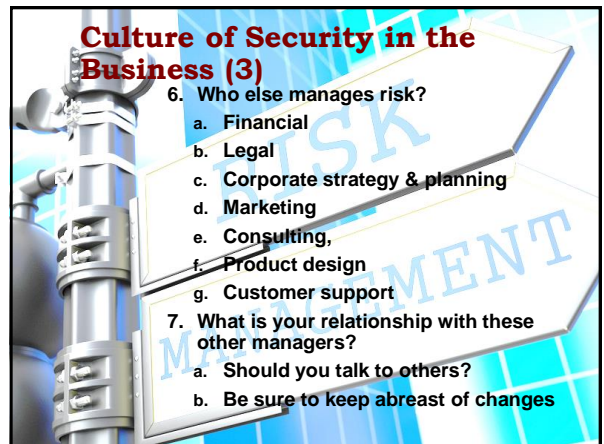
## Culture of Security in the Business (2)

- Questions cont'd
- 3. Relevant regulations & statutes: inventory & understanding (more complex in international organizations)
- 4. Influence / awareness of public opinion: function of public visibility; may involve marketing functions
- 5. Risk to reputation: consumer confidence; transparency acceptable / useful?



## Culture of Security in the Business (3)

6. Who else manages risk?
  - a. Financial
  - b. Legal
  - c. Corporate strategy & planning
  - d. Marketing
  - e. Consulting,
  - f. Product design
  - g. Customer support
7. What is your relationship with these other managers?
  - a. Should you talk to others?
  - b. Be sure to keep abreast of changes



## Alliance with Corporate & Outside Counsel

- Coordinate w/ counsel
  - ❑ Policy
  - ❑ Investigations
  - ❑ Contracts
  - ❑ Incidents
- Intellectual property issues must involve counsel
- Maintain close ties



37

Copyright©2014 M. E. Kabay. All rights reserved.

## Partnership with Internal Audit

- Close partnership essential
- CISO must ensure smooth collaboration
  - ❑ Standard of care requires demonstration of effective functioning of controls
  - ❑ Work together on monitoring & reporting
  - ❑ Ensure full access to information security processes
  - ❑ Provide support to each other in escalation
- Focus on egoless work\*:
  - ❑ Audit results are positive contribution to continuous process improvement
  - ❑ Findings never interpreted as personal attacks
  - ❑ Constructive criticisms welcomed, praised & rewarded



\*See Kabay, M. (2009), "On Writing" v10, Section 9, "Egoless Work." < <http://www.mekabay.com/methodology/writing.pdf> >

38

## Tension with IT

- Some CISOs report to CIO (head of IT)
  - ❑ Potential conflict of interest
  - ❑ Scope of CISO's work extends beyond IT
  - ❑ Impression that CISO is *IT security* manager instead of *information security* manager
- Mistake to fund CISO out of IT budget
  - ❑ Inappropriate allocation of costs
  - ❑ Can hit IT hard & cause resentment
- CISO should report to Board like all other C-levels
  - ❑ But important not to lose collaboration with IT
  - ❑ If impossible & CISO reports to CIO, try dotted-line relationships to senior executives (difficult)



39

Copyright©2014 M. E. Kabay. All rights reserved.

## Organizational Structure

- Reporting (discussed on previous slide)
  - ❑ Note also that some CISOs report to CEO, COO or CFO
- Other possibilities
  - ❑ Some CISOs responsible for
    - ✓ Physical security
    - ✓ Executive protection
  - ❑ Collaborate closely with physical security chief

### Key elements of CISO role

- Governance
- Policy management
- Compliance monitoring & reporting
- Parameters for IT security operations
- Information security investigations
- Forensics & incident handling
- Identity & access management
- Business continuity
- Records management
- E-discovery

40

Copyright©2014 M. E. Kabay. All rights reserved.

## Additional Roles Beyond Internal Responsibilities

- Share what's experienced
- Codify security practice
- Improve understanding of security
- Participate in professional organizations
- Write for professional publications
- Speak to community / professional / trade organizations
- Eliminate confusion
- Define role in everyone's minds



41

Copyright©2014 M. E. Kabay. All rights reserved.

# DISCUSSION

42

Copyright©2014 M. E. Kabay. All rights reserved.