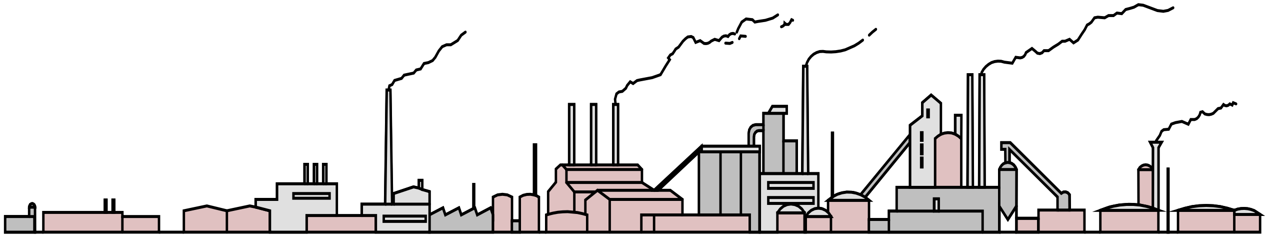
HUMAN FACTORS IN INDUSTRIAL CYBER SECURITY

by Paul Baybutt, Primatech Inc.

Presented at the ISA Industrial Network and Systems Security Symposium, Houston, October, 2004

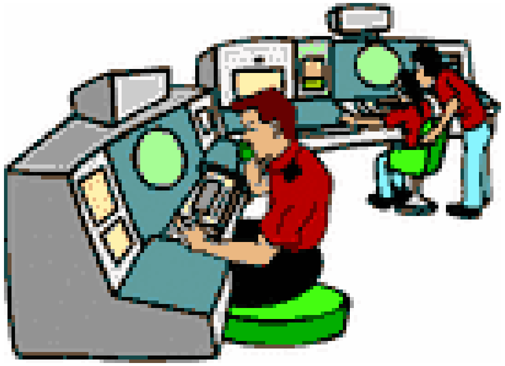
paulb@primatech.com

www.primatech.com



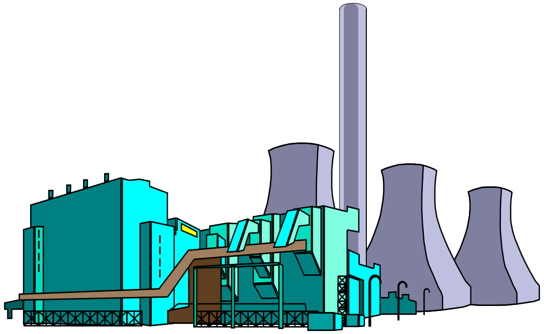
OVERVIEW

- Meaning of industrial cyber security and the protection of computer systems
- Meaning and importance of human factors for cyber security
- Addressing human factors for cyber security



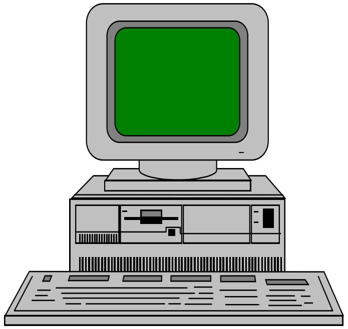
CYBER SECURITY FOR MANUFACTURING AND PROCESS PLANTS

- Protection of manufacturing and process plant computer systems from:
  - Access by adversaries who want to obtain, corrupt, damage, destroy or prohibit access to valuable information
  - Cyber or physical attack by adversaries who wish to disable or manipulate them to cause harm



PROTECTION OF COMPUTER SYSTEMS

- Computer systems consist of:



Hardware

Software

Peopleware

- Any system is only as strong as its weakest link

SOME ISSUES WITH PEOPLE

- Prone to slips and mistakes
- Mindsets and habits
- Forgetful
- Inconsistent behavior
- Do not always follow policies and procedures
- Willful

“Man is a creature made at the end of the week ... when God was tired”

- Mark Twain

WHAT PEOPLE ARE INVOLVED?

- Designers
- Developers
- Manufacturers
- Installers and integrators
- Operators
- Users
- Maintainers
- Administrators

FAILURES OF PEOPLE

Type	**Meaning**
Omission error	Action is not performed
Commission error	Action is performed incorrectly
Extraneous act	Non-required action is performed instead of or in addition to required act
Violations (deliberate acts)	Action that is prohibited, or different from that prescribed

WHY ARE THERE PEOPLE FAILURES?

- The likelihood of human failures is influenced by a variety of factors, e.g.
  - Time pressures
  - Resource constraints
  - Adequacy of training
  - Awareness of cyber security matters
  - Suitability of the environment
  - Organization
  - System design

EXAMPLES OF HUMAN FAILURES/FACTORS

- Design
  - Software flaws
- Development
  - Backdoors and logic bombs
- Installation
  - Default configurations not changed
  - Security systems not enabled or disabled
- Use
  - Policies not followed for passwords
  - Unauthorized modem installation
  - Disclosure of sensitive information
  - Inadvertent installation of malware
- Maintenance
  - Patches and updates not installed
  - Poor account management

HOW CAN HUMAN FACTORS BE ADDRESSED FOR CYBER SECURITY?

- Recognize their importance!
- Understand cyber vulnerabilities
- Identify aspects of cyber security influenced by human factors
- Perform human factors analysis

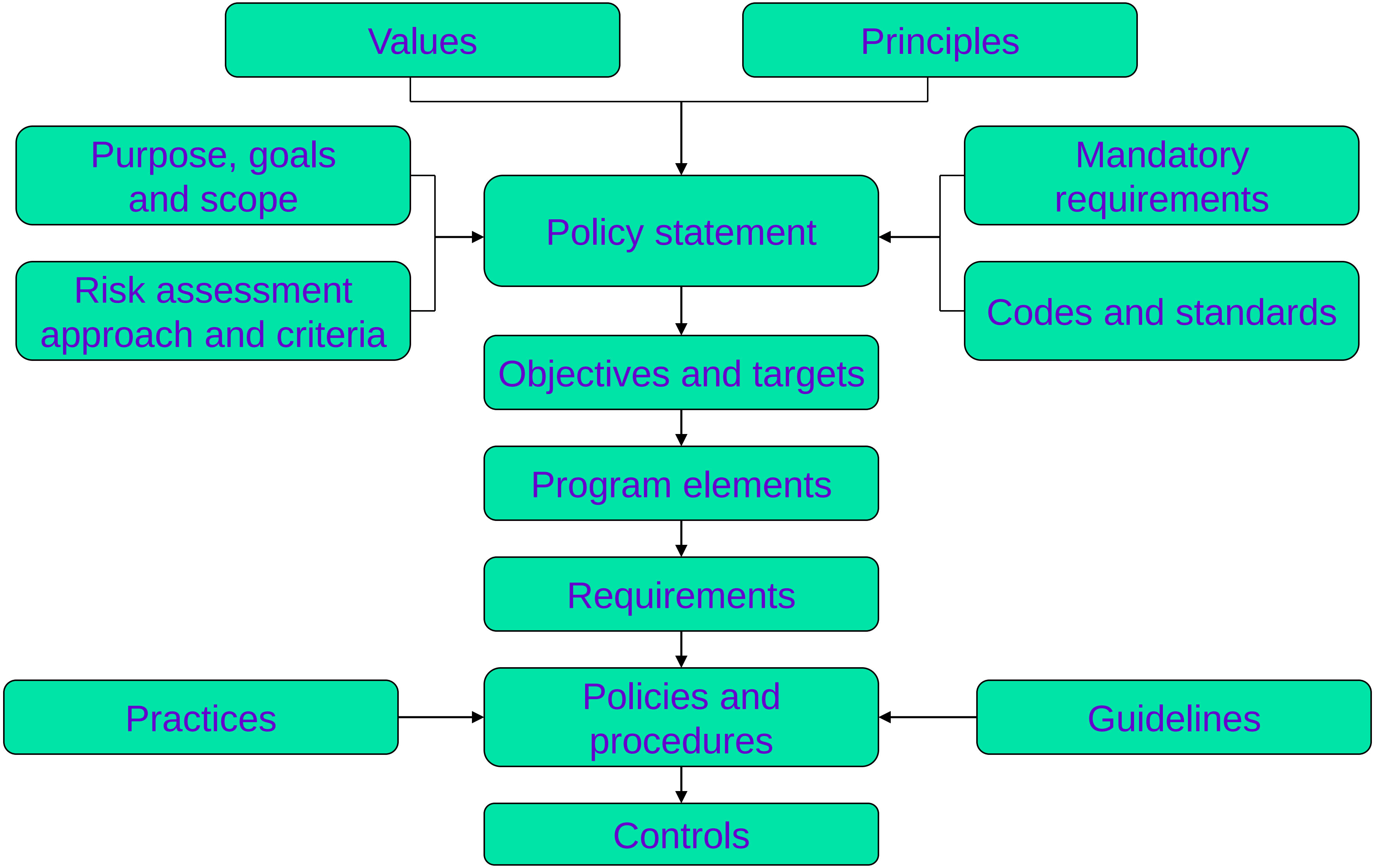
IDENTIFY ASPECTS OF CYBER SECURITY

- Determine approach being used for cyber security
  - Code of practice for controls, e.g. ISO 17799
  - Cyber security program, e.g. ISA SP99
  - Cyber security management system (CSMS), BS 7799:2, CIDX CSMS

IDENTIFY ASPECTS OF CYBER SECURITY (CONTD.)

- Determine human involvement with each part of the system you are using

ENTITIES IN A MANAGEMENT SYSTEM



Values

Principles

Purpose, goals and scope

Risk assessment approach and criteria

Policy statement

Mandatory requirements

Codes and standards

Objectives and targets

Program elements

Requirements

Practices

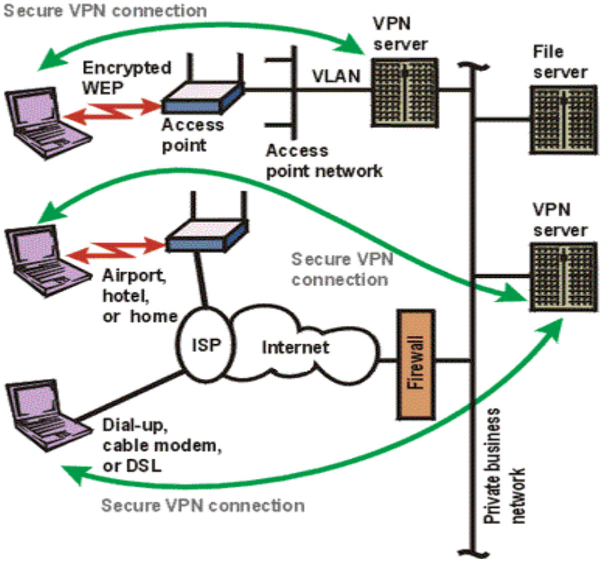
Policies and procedures

Guidelines

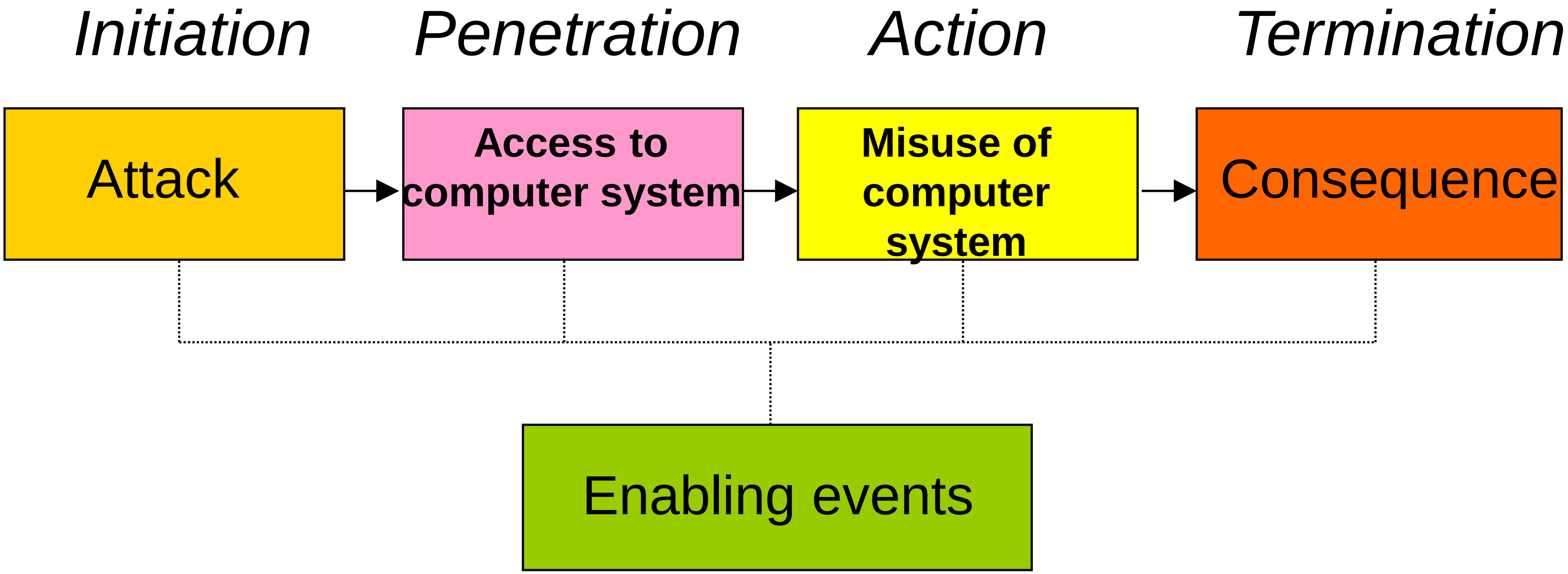
Controls

PERFORM HUMAN FACTORS ANALYSIS

- Address human factors in:
  - Risk assessment of cyber threats
  - Cyber security management system

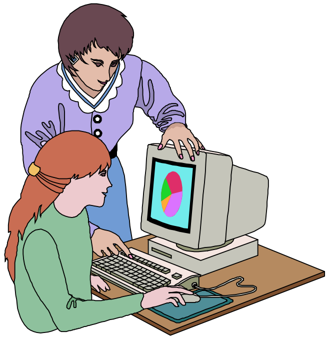


HUMAN FACTORS ANALYSIS IN RISK ASSESSMENT



HUMAN FACTORS ANALYSIS FOR THE CSMS

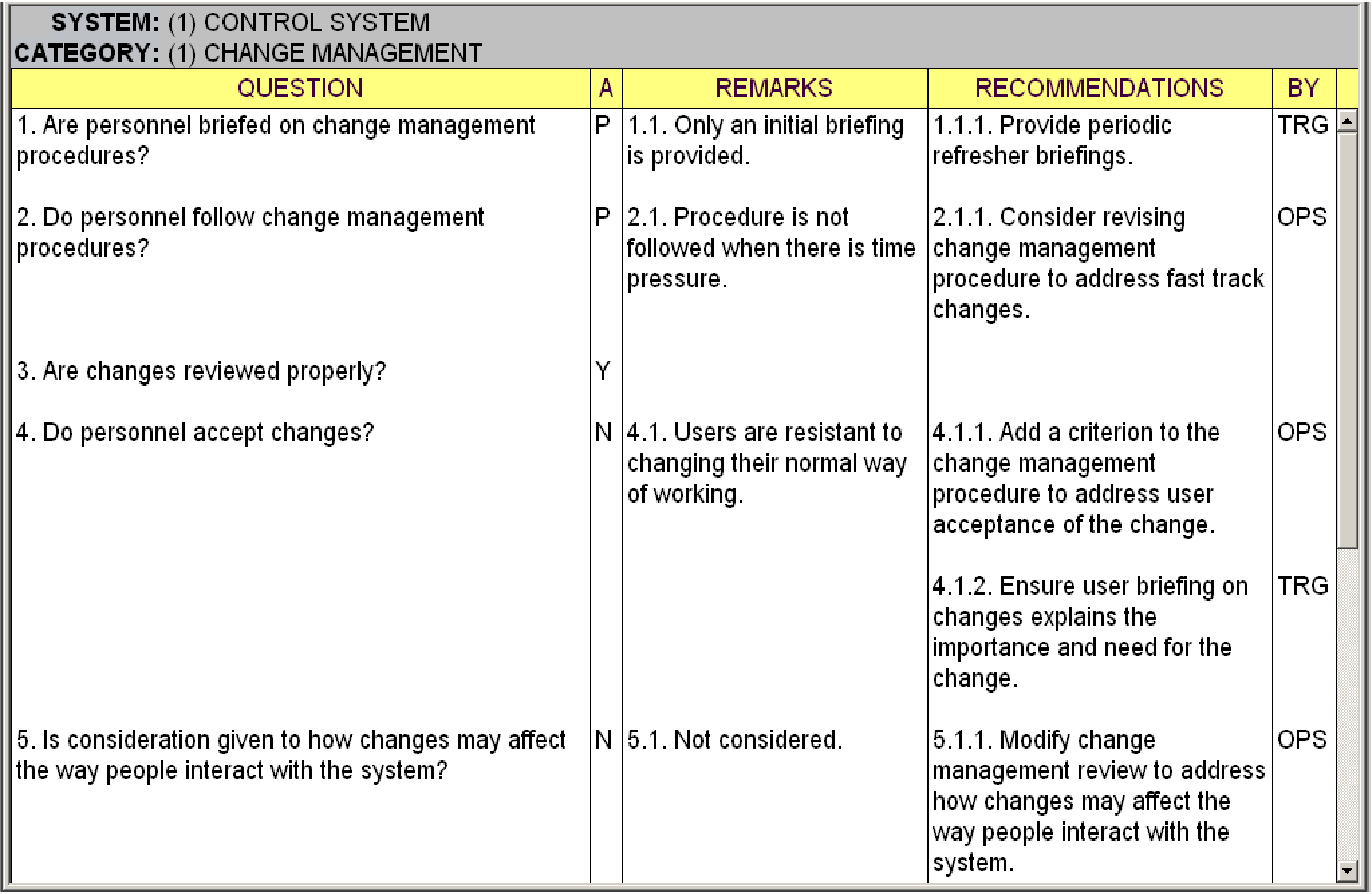
- For each part of the cyber security management system identify:
  - Possible failures and the principal factors that may influence them
  - Potential corrective actions depending on the likelihood, consequences and safeguards against the failures



HUMAN FACTORS ANALYSIS METHODS

- Checklists
- Task analysis

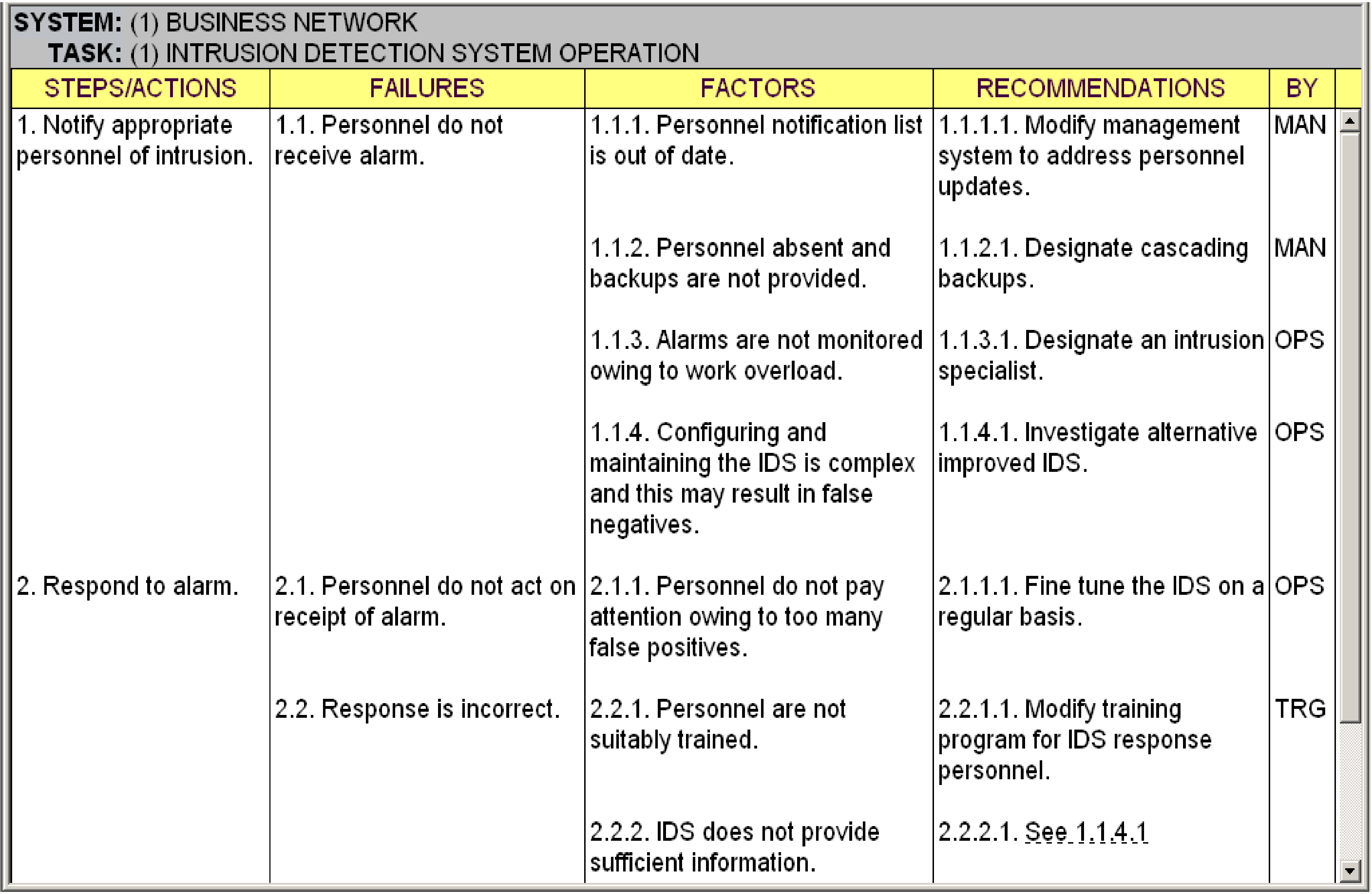
CHECKLIST EXAMPLE



SYSTEM: (1) CONTROL SYSTEM
CATEGORY: (1) CHANGE MANAGEMENT

QUESTION	A	REMARKS	RECOMMENDATIONS	BY
1. Are personnel briefed on change management procedures?	P	1.1. Only an initial briefing is provided.	1.1.1. Provide periodic refresher briefings.	TRG
2. Do personnel follow change management procedures?	P	2.1. Procedure is not followed when there is time pressure.	2.1.1. Consider revising change management procedure to address fast track changes.	OPS
3. Are changes reviewed properly?	Y			
4. Do personnel accept changes?	N	4.1. Users are resistant to changing their normal way of working.	4.1.1. Add a criterion to the change management procedure to address user acceptance of the change.	OPS
			4.1.2. Ensure user briefing on changes explains the importance and need for the change.	TRG
5. Is consideration given to how changes may affect the way people interact with the system?	N	5.1. Not considered.	5.1.1. Modify change management review to address how changes may affect the way people interact with the system.	OPS

TASK ANALYSIS EXAMPLE

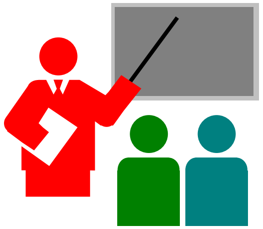


SYSTEM: (1) BUSINESS NETWORK
TASK: (1) INTRUSION DETECTION SYSTEM OPERATION

STEPS/ACTIONS	FAILURES	FACTORS	RECOMMENDATIONS	BY
1. Notify appropriate personnel of intrusion.	1.1. Personnel do not receive alarm.	1.1.1. Personnel notification list is out of date.	1.1.1.1. Modify management system to address personnel updates.	MAN
		1.1.2. Personnel absent and backups are not provided.	1.1.2.1. Designate cascading backups.	MAN
		1.1.3. Alarms are not monitored owing to work overload.	1.1.3.1. Designate an intrusion specialist.	OPS
		1.1.4. Configuring and maintaining the IDS is complex and this may result in false negatives.	1.1.4.1. Investigate alternative improved IDS.	OPS
2. Respond to alarm.	2.1. Personnel do not act on receipt of alarm.	2.1.1. Personnel do not pay attention owing to too many false positives.	2.1.1.1. Fine tune the IDS on a regular basis.	OPS
	2.2. Response is incorrect.	2.2.1. Personnel are not suitably trained.	2.2.1.1. Modify training program for IDS response personnel.	TRG
		2.2.2. IDS does not provide sufficient information.	2.2.2.1. See 1.1.4.1	

HARDENING SYSTEMS AGAINST PEOPLE FAILURES

- Design systems with human factors in mind
  - E.g. policies and procedures
- Provide training and awareness
  - Including refreshers and reminders
- Provide backups to people
  - Independent and redundant
- Conduct audits regularly

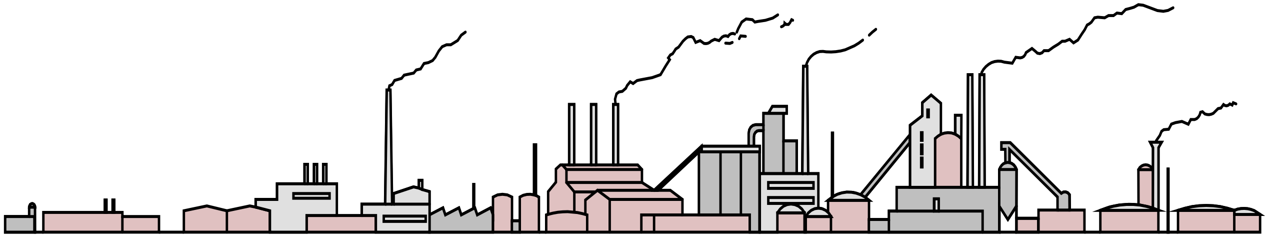


“The only real mistake is the one from which we learn nothing.”

John Powell

SUMMARY

- Human factors issues dominate cyber security risk
- Approaches are available for addressing human factors
- They should be applied to all aspects of the cyber security management system



FURTHER INFORMATION

- Technical papers on cyber and process security:
  - www.primatech.com
- Contact info:
  - paulb@primatech.com