GJØVIK UNIVERSITY COLLEGE

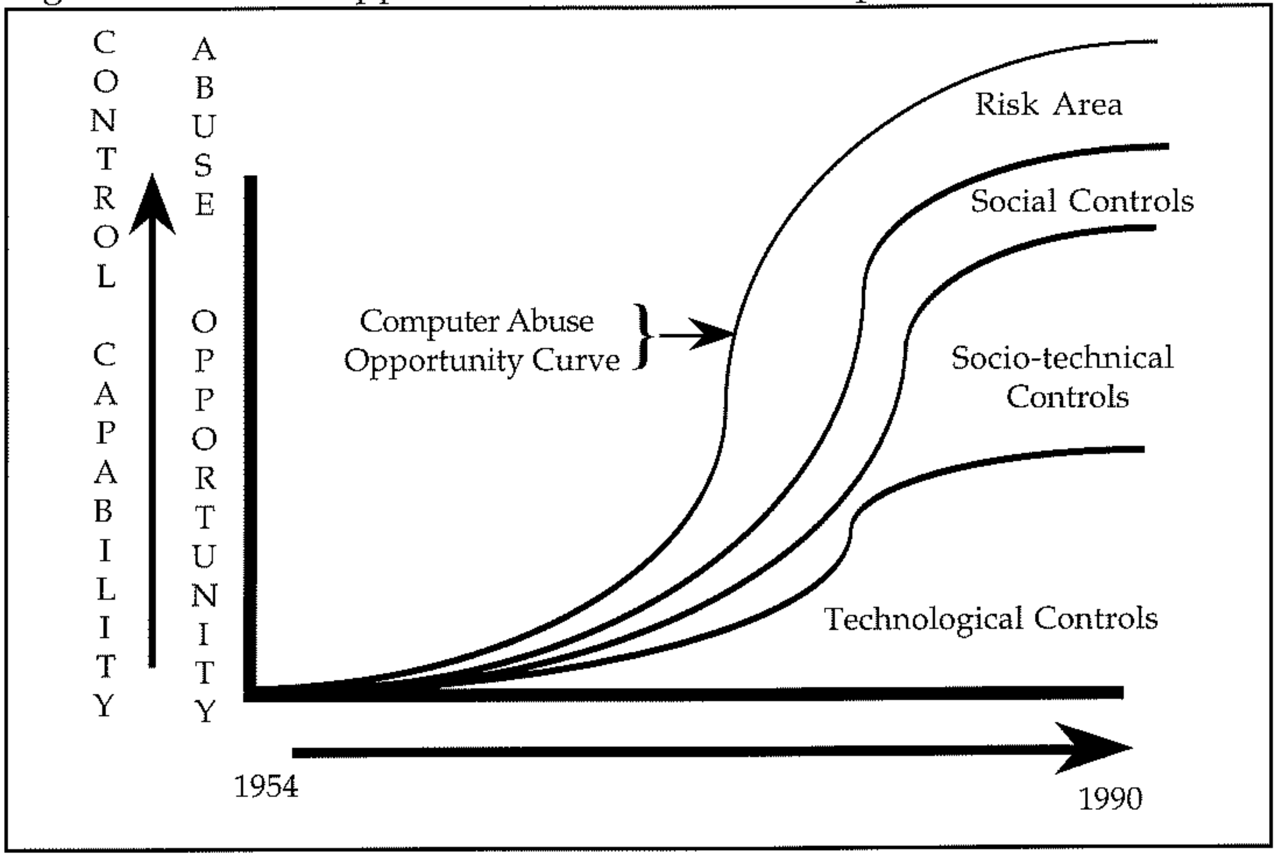
Mind the Gap

Modeling Cyber Security Governance from developing to developing nations : The continous need for more education to fill the control gap.

Professor Dr. Stewart Kowalski
Vice Dean of Education
Faculty of Computer and Media Technology
Norwegian Information Security Lab (NISlab)
Center for Cyber and Information Security

Questions: Why is there a Security GAP in developing countries?

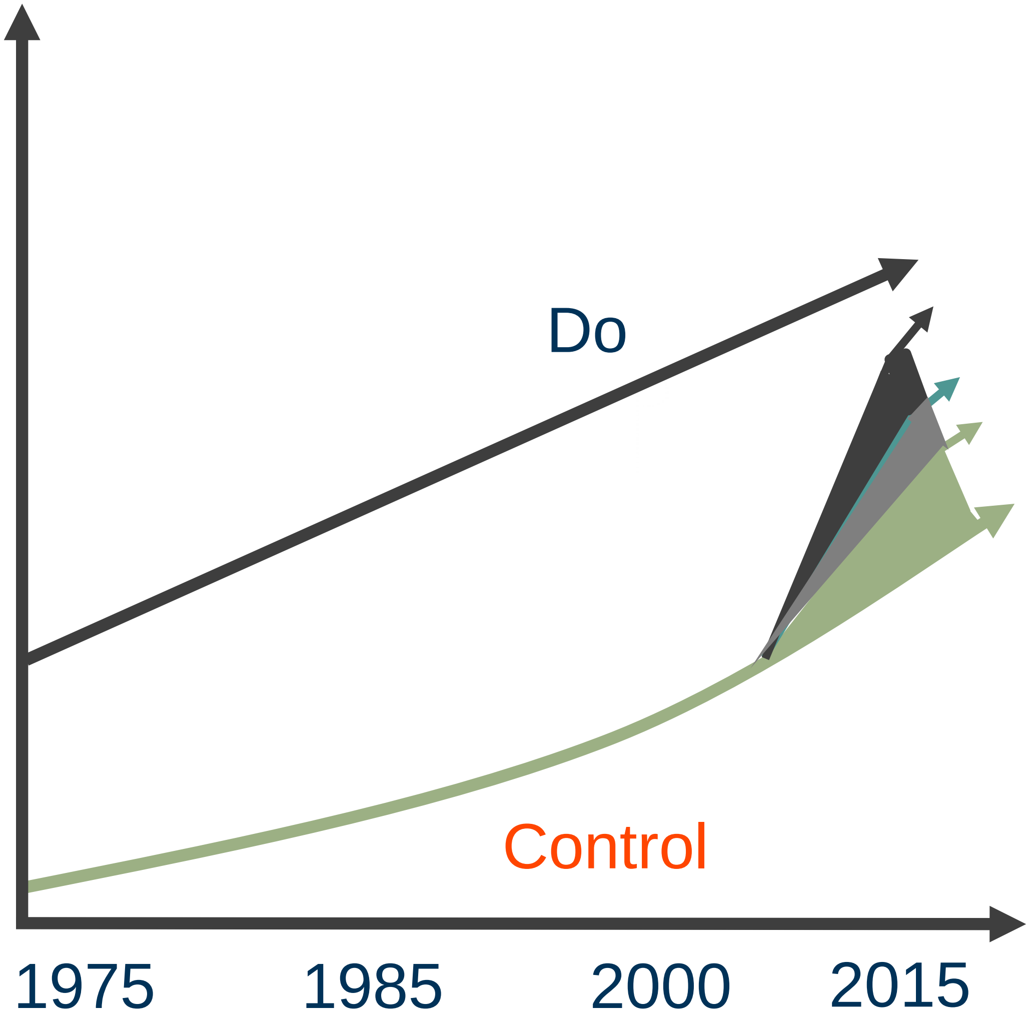
Figure 3.1 Abuse Opportunities and Control Capabilities vs. Time



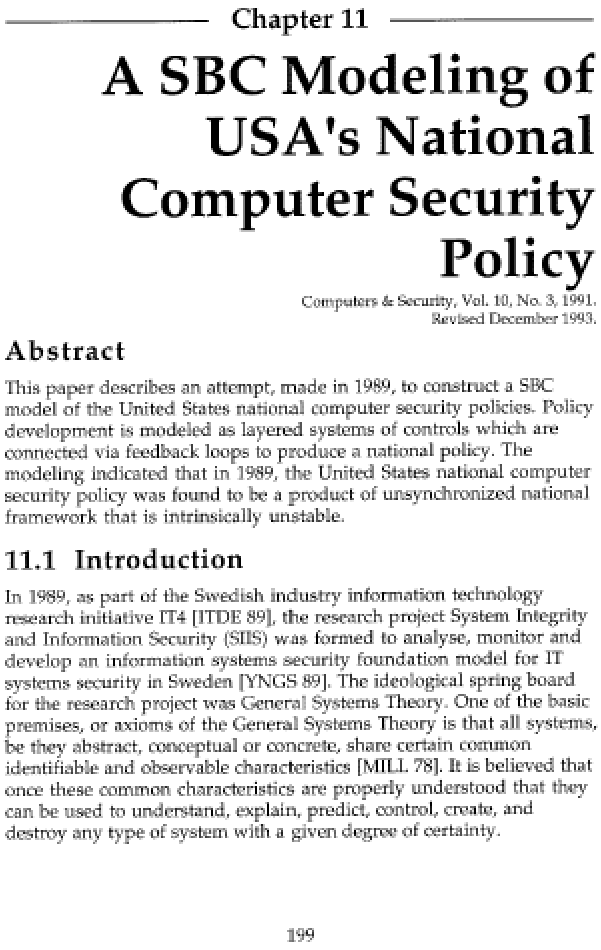
Answer: There is always a Security GAP with new technology !

THE PROBLEM NEED TO FILL THE GAP

- Technology
  - Secure Information Environment
- Processes
  - Information Security Managment System
- People
  - Culture and Awareness and competence



1989 USA SITUATION NOT IDEAL (SWEDEN CAN LEARN A LOT FROM THE AMERICAN MISTAKES)



Chapter 11

A SBC Modeling of USA's National Computer Security Policy

Computers & Security, Vol. 10, No. 3, 1991.
Revised December 1993.

Abstract

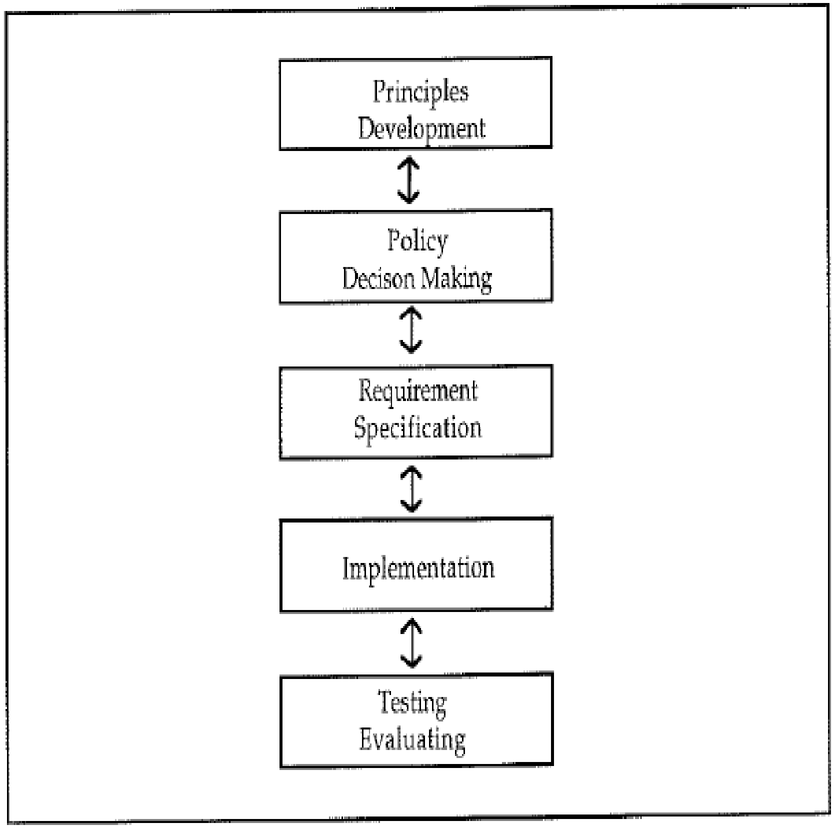
This paper describes an attempt, made in 1989, to construct a SBC model of the United States national computer security policies. Policy development is modeled as layered systems of controls which are connected via feedback loops to produce a national policy. The modeling indicated that in 1989, the United States national computer security policy was found to be a product of unsynchronized national framework that is intrinsically unstable.

11.1 Introduction

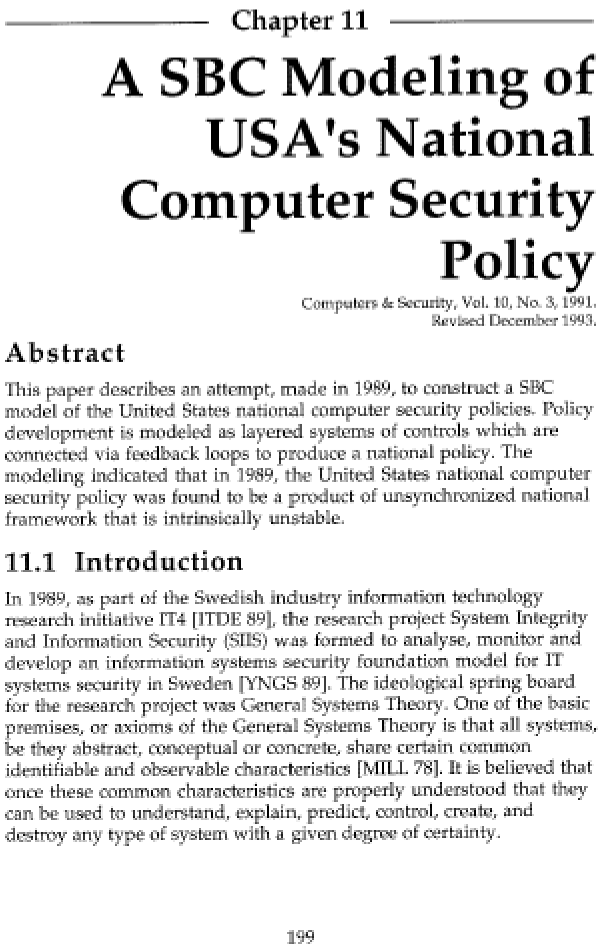
In 1989, as part of the Swedish industry information technology research initiative IT4 [ITDE 89], the research project System Integrity and Information Security (SIIS) was formed to analyse, monitor and develop an information systems security foundation model for IT systems security in Sweden [YNGS 89]. The ideological spring board for the research project was General Systems Theory. One of the basic premises, or axioms of the General Systems Theory is that all systems, be they abstract, conceptual or concrete, share certain common identifiable and observable characteristics [MILL 78]. It is believed that once these common characteristics are properly understood that they can be used to understand, explain, predict, control, create, and destroy any type of system with a given degree of certainty.

199

Figure 11.1 The Ideal National Computer Security Policy Design Model [Source WARE 89].



1989 USA SITUATION NOT IDEAL
(SWEDEN CAN LEARN A LOT FROM THEIR MISTAKES)



Chapter 11

A SBC Modeling of USA's National Computer Security Policy

Computers & Security, Vol. 10, No. 3, 1991.
Revised December 1993.

Abstract

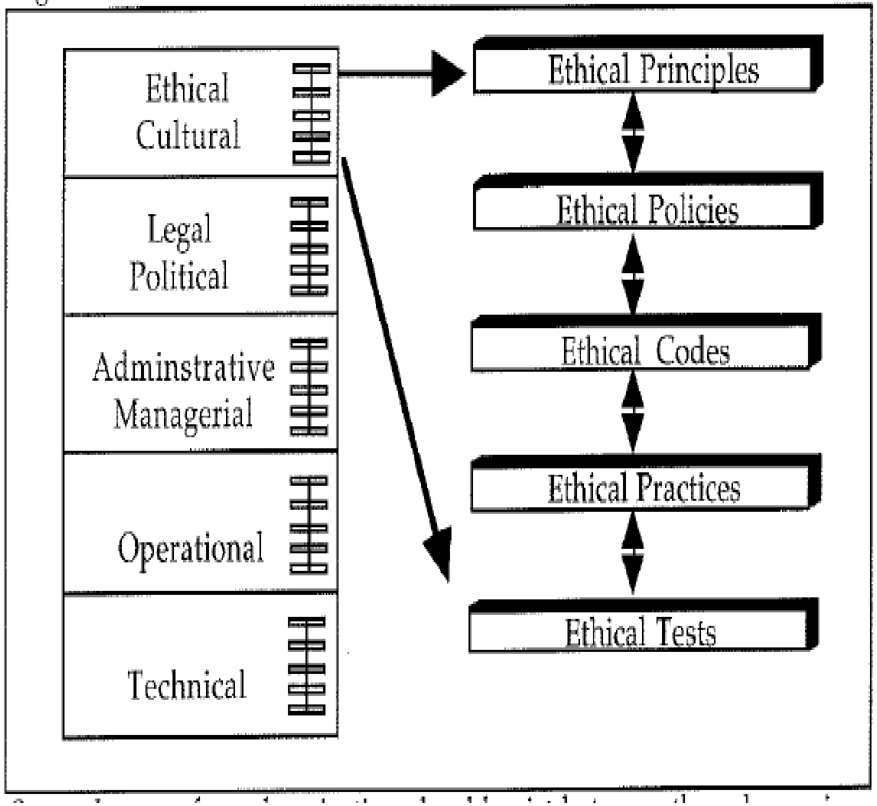
This paper describes an attempt, made in 1989, to construct a SBC model of the United States national computer security policies. Policy development is modeled as layered systems of controls which are connected via feedback loops to produce a national policy. The modeling indicated that in 1989, the United States national computer security policy was found to be a product of unsynchronized national framework that is intrinsically unstable.

11.1 Introduction

In 1989, as part of the Swedish industry information technology research initiative IT4 [ITDE 89], the research project System Integrity and Information Security (SIIS) was formed to analyse, monitor and develop an information systems security foundation model for IT systems security in Sweden [YNGS 89]. The ideological spring board for the research project was General Systems Theory. One of the basic premises, or axioms of the General Systems Theory is that all systems, be they abstract, conceptual or concrete, share certain common identifiable and observable characteristics [MILL 78]. It is believed that once these common characteristics are properly understood that they can be used to understand, explain, predict, control, create, and destroy any type of system with a given degree of certainty.

199

Figure 11.4 Combined Static and Process Meta Model



CHAPTER 11-12 USING THE SBC MODELING THE WORLD, FROM IDEAL TO ACTUAL!!

Ideal

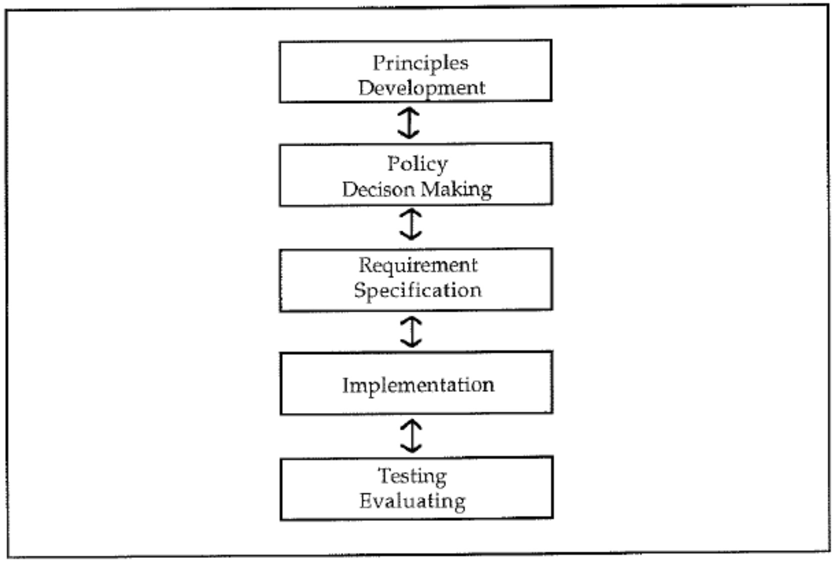
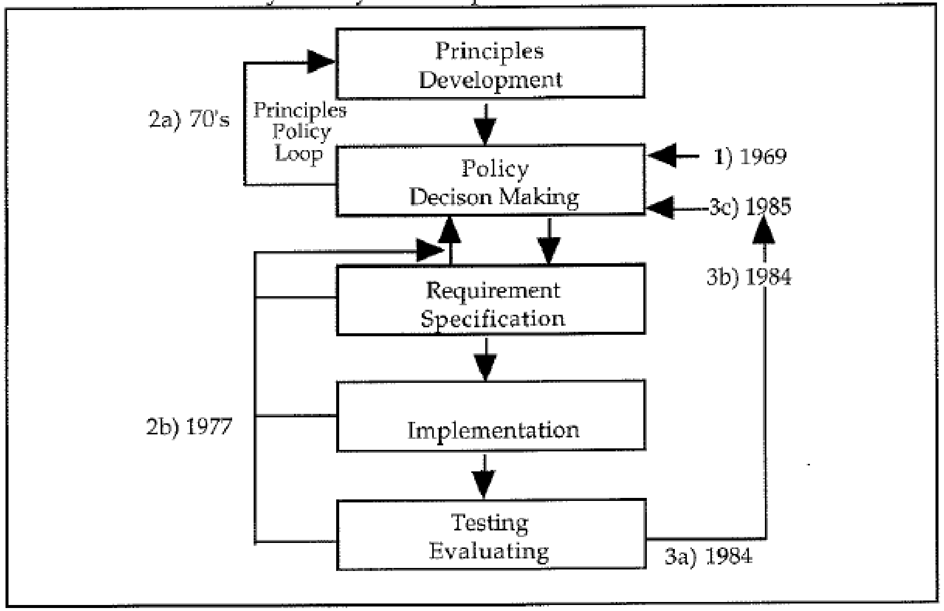


Figure 11.2 Process Meta Model of the U.S.A National Computer Security Policy Development 1969-1985



FROM IDEAL TO ACTUAL!!

Figure 12.3 SBC Flow Diagram Ethical Subsystem

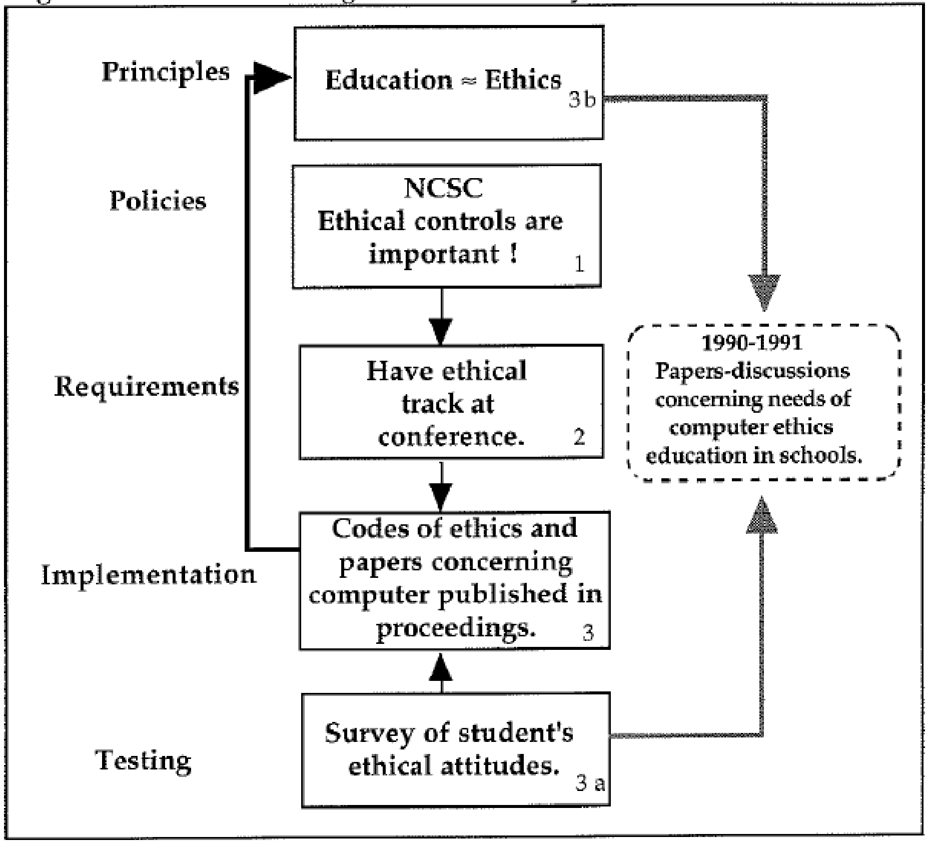
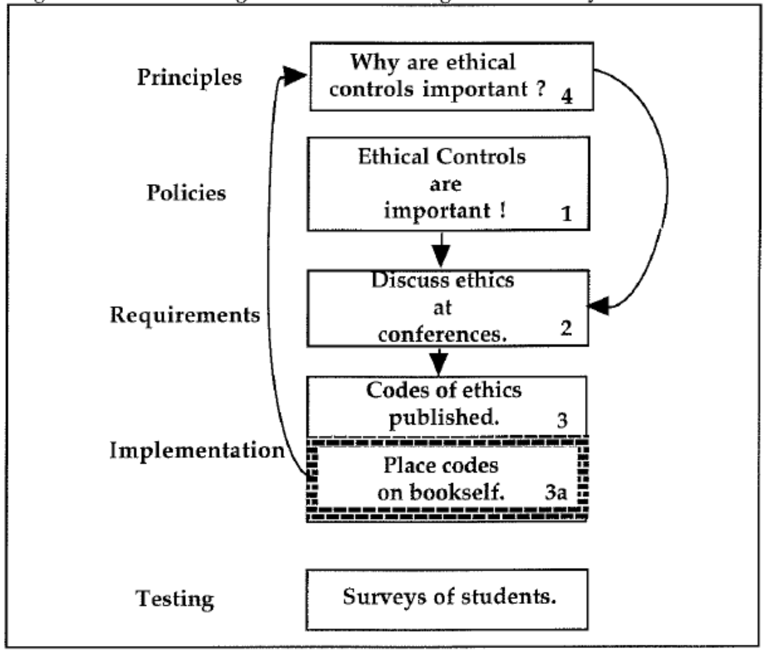

Principles
Policies
Requirements
Implementation
Testing
Education ≈ Ethics 3b
NCSC
Ethical controls are important ! 1
Have ethical track at conference. 2
Codes of ethics and papers concerning computer published in proceedings. 3
Survey of student's ethical attitudes. 3 a
1990-1991
Papers-discussions concerning needs of computer ethics education in schools.

Figure 12.4 Flow Diagram Disfunctioning Ethical Subsystem


Principles
Policies
Requirements
Implementation
Testing
Why are ethical controls important ? 4
Ethical Controls are important ! 1
Discuss ethics at conferences. 2
Codes of ethics published. 3
Place codes on bookself. 3a
Surveys of students.

, FROM IDEAL TO ACTUAL!!

Figure 12.5 Flow Diagram Political Legal Subsystem

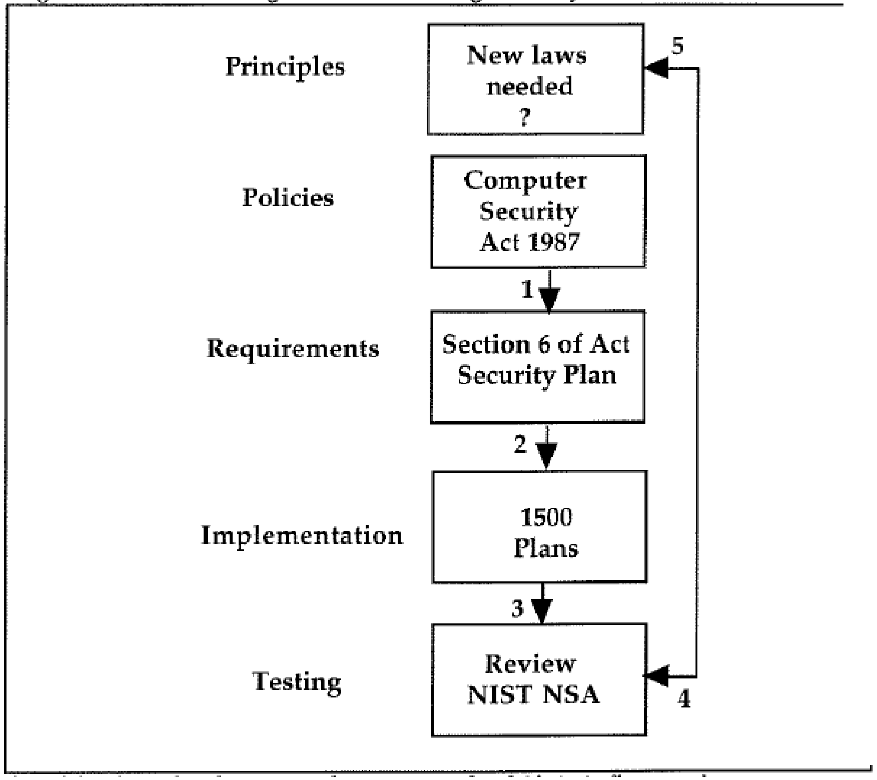
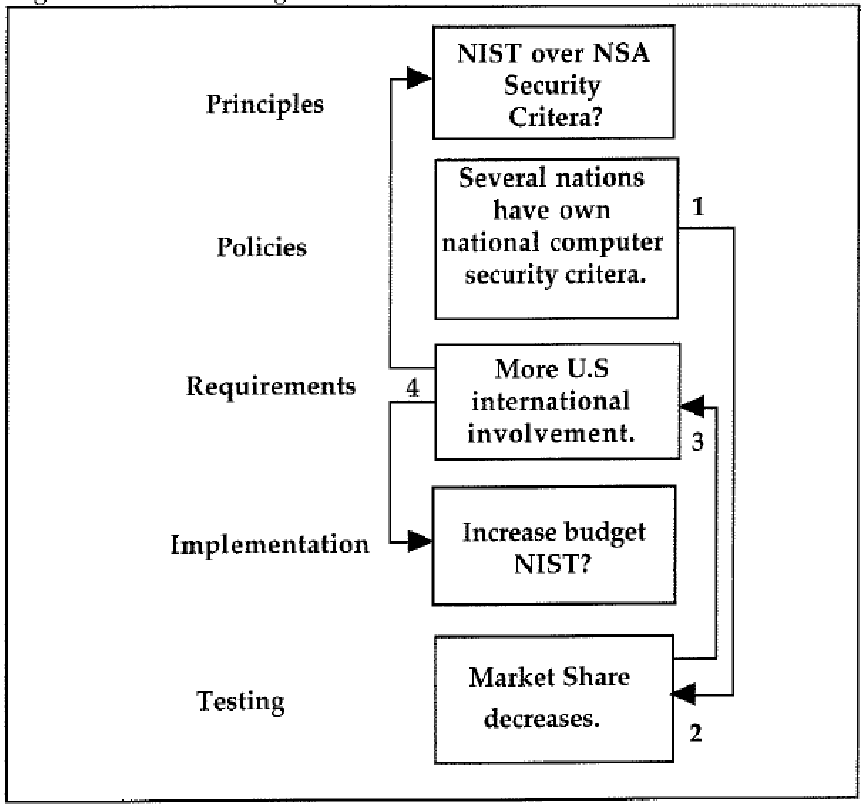


Figure 12.6 Flow Diagram of a Possible Future Political Situation


Principles
Policies
Requirements
Implementation
Testing
NIST over NSA Security Critera?
Several nations have own national computer security critera.
More U.S international involvement.
Increase budget NIST?
Market Share decreases.
1
2
3
4

FROM IDEAL TO ACTUAL!!

Figure 12.8 Flow Diagram Disfunctioning Operational Subsystem.

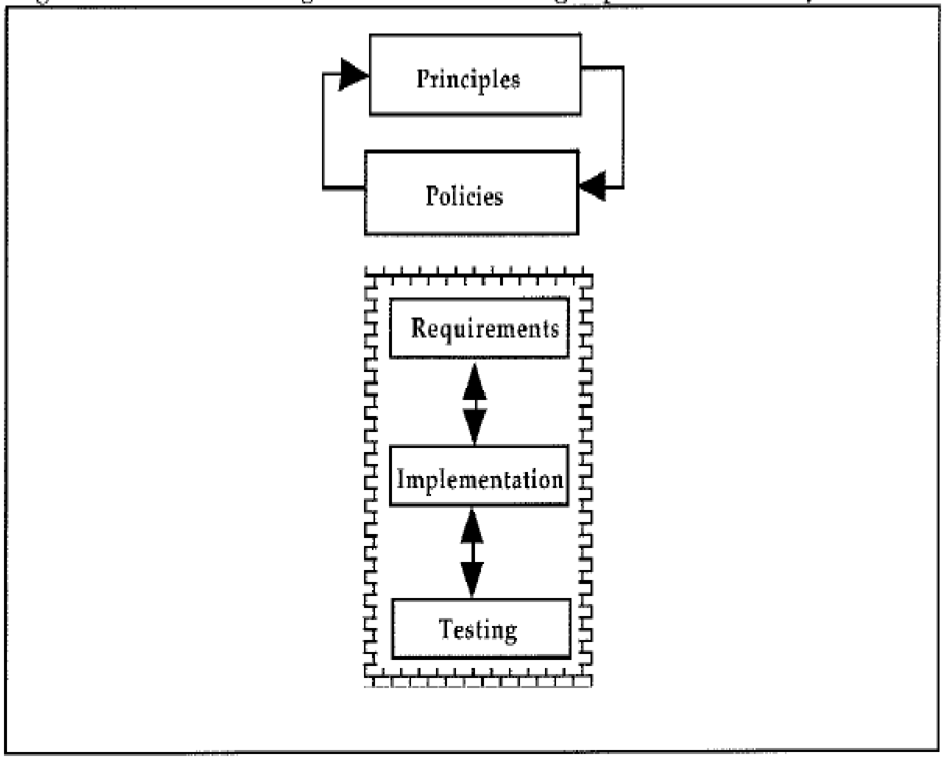
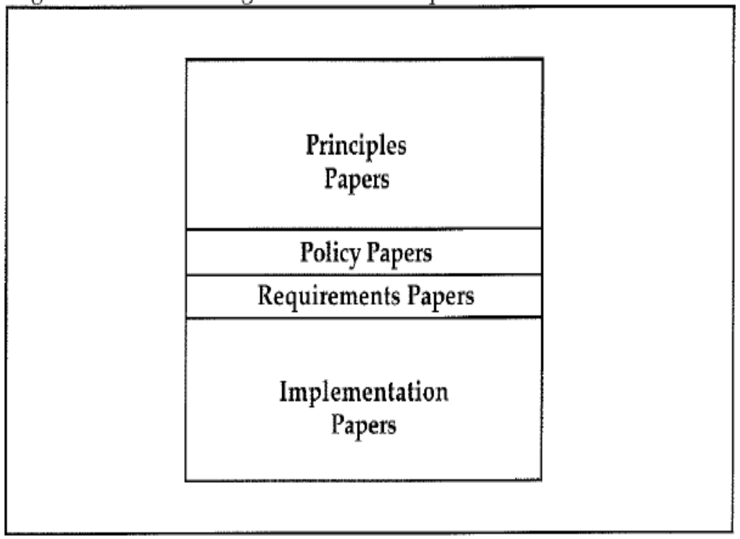
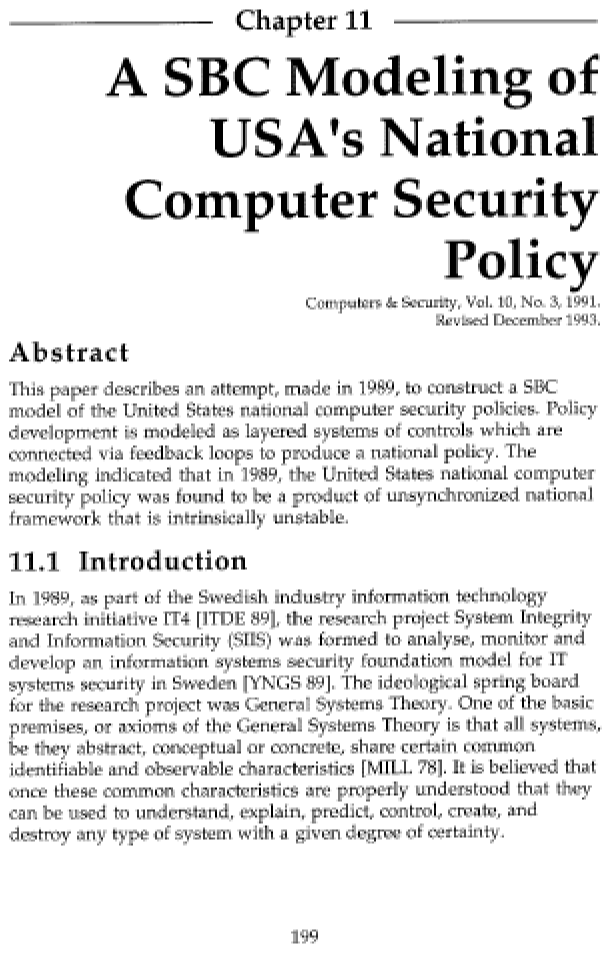


Figure 12.9 Block Diagram Technical Papers



1989 USA COMPUTER SECURITY SITUATION NOT IDEAL (SWEDEN CAN LEARN A LOT FROM THEIR MISTAKES)



Chapter 11

A SBC Modeling of USA's National Computer Security Policy

Computers & Security, Vol. 10, No. 3, 1991.
Revised December 1993.

Abstract

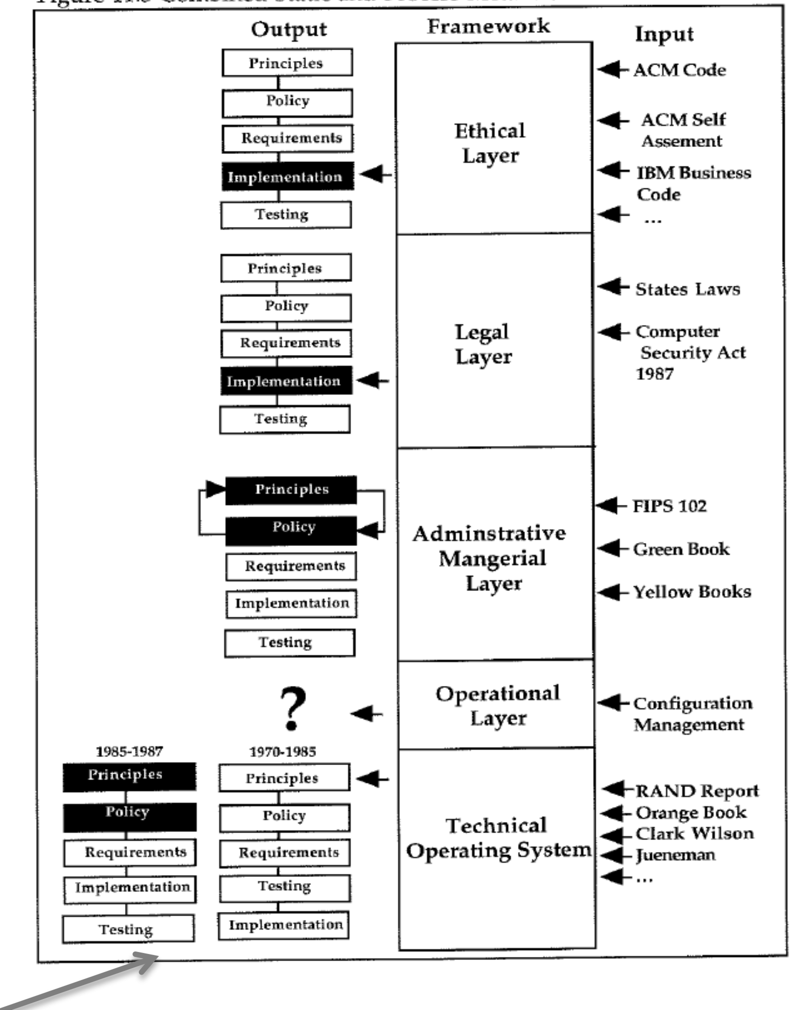
This paper describes an attempt, made in 1989, to construct a SBC model of the United States national computer security policies. Policy development is modeled as layered systems of controls which are connected via feedback loops to produce a national policy. The modeling indicated that in 1989, the United States national computer security policy was found to be a product of unsynchronized national framework that is intrinsically unstable.

11.1 Introduction

In 1989, as part of the Swedish industry information technology research initiative IT4 [ITDE 89], the research project System Integrity and Information Security (SIIS) was formed to analyse, monitor and develop an information systems security foundation model for IT systems security in Sweden [YNGS 89]. The ideological spring board for the research project was General Systems Theory. One of the basic premises, or axioms of the General Systems Theory is that all systems, be they abstract, conceptual or concrete, share certain common identifiable and observable characteristics [MILL 78]. It is believed that once these common understood that they can be used to understand, explain, predict, control, create, and destroy any type of system with a given degree of certainty.

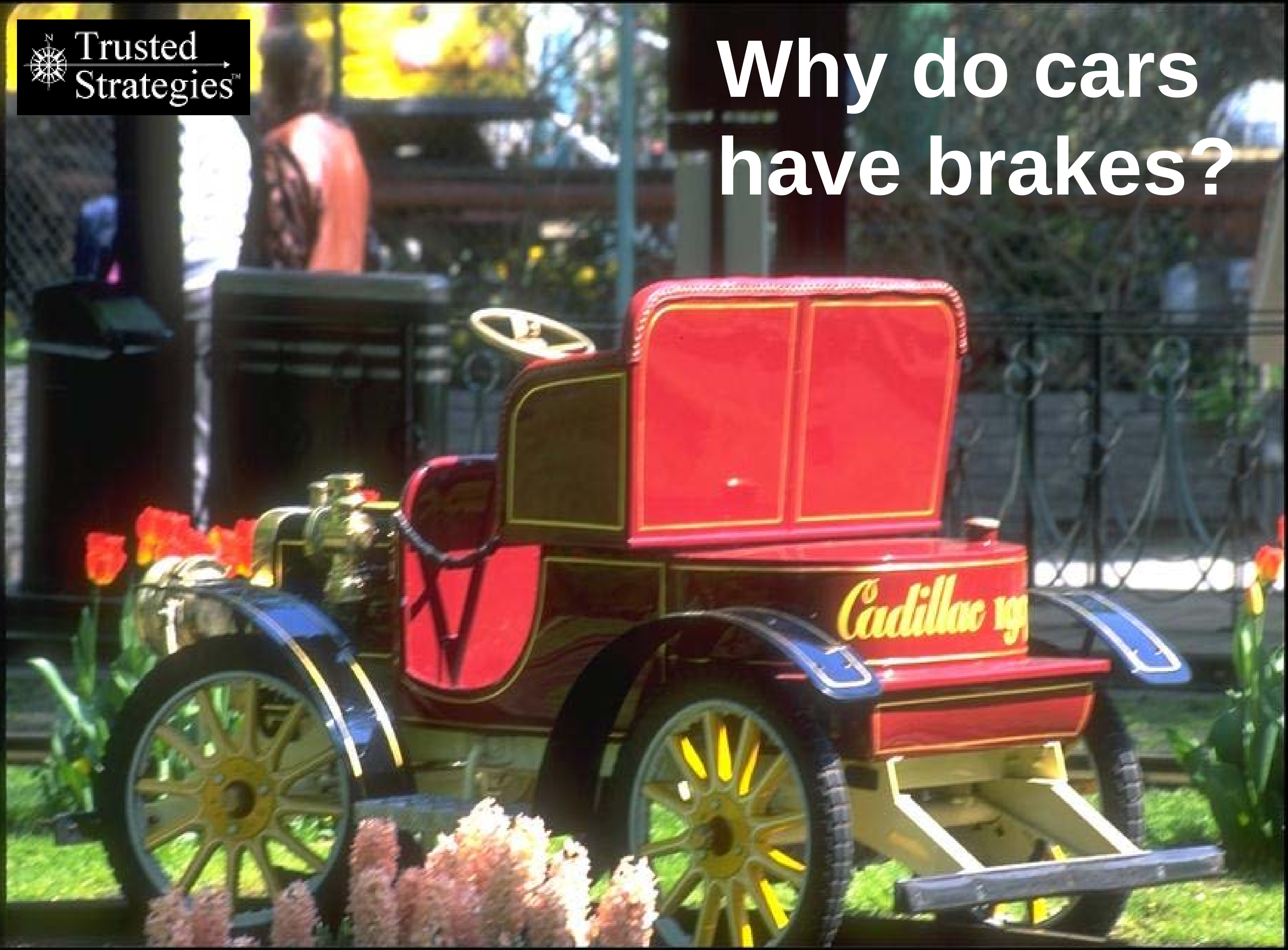
199

Figure 11.5 Combined Static and Process Meta Model U.S.A. 1989



Systemic Gap we need to learn faster with faster technology!

Why do cars have brakes?

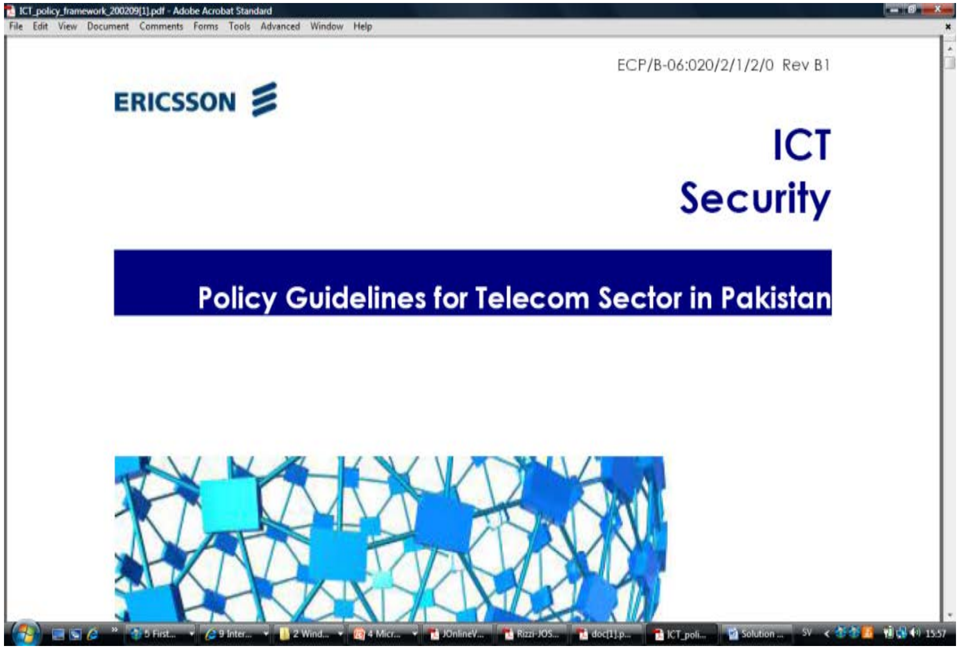


So they can go ***FASTER!!!***

Without proper controls & safeguards, it’s dangerous to flex your muscles

Industrial Model

Islamabad November 25, 2008 : Chairman Pakistan Telecommunication Authority (PTA), Dr.Mohammed Yaseen chairing a meeting of Expert Group Forum on Information Security Guidelines held at PTA Headquarters.



ECP/B-06:020/2/1/2/0 Rev B1

ERICSSON

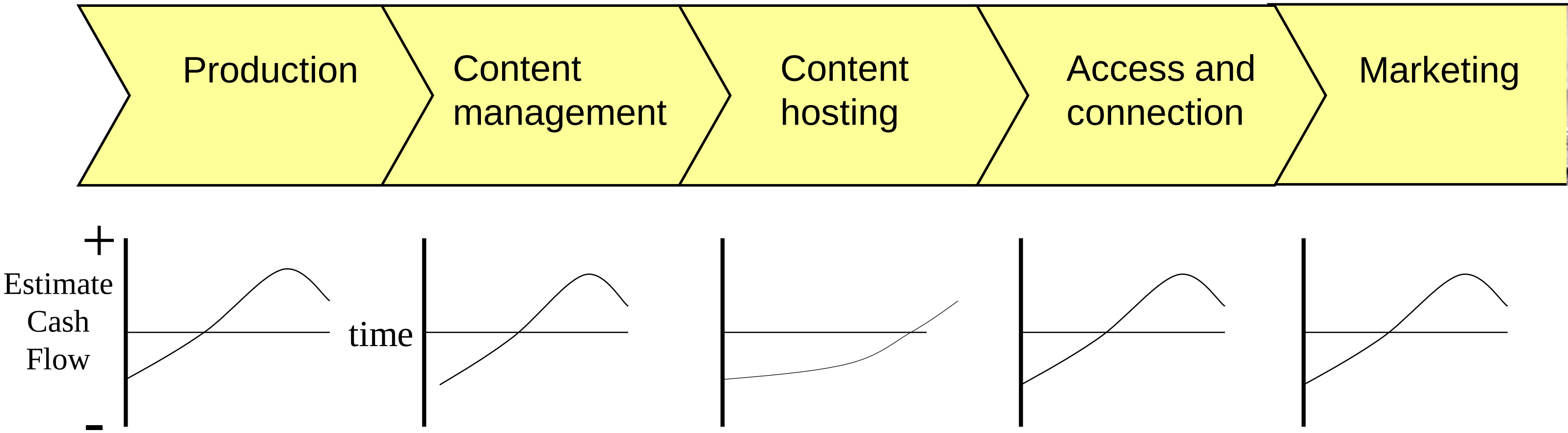
ICT
Security

Policy Guidelines for Telecom Sector in Pakistan

A Value Chain is

- A Value Chain is
  - the interconnect group of industry participants that collectively create value for the end user.
  - If technologies or services are to succeed they must deliver financial or operational value at every stage of the chain.
  - For any technology or service to be adopted, each element on the chain must add value for the next element.
  - (The strategic Implications of Computing and the Internet on Wireless: The Competitive Blur Through 2008, Herschel Schoteck Associates.)

Example of Mobile Content Value Chain.



Production

Content management

Content hosting

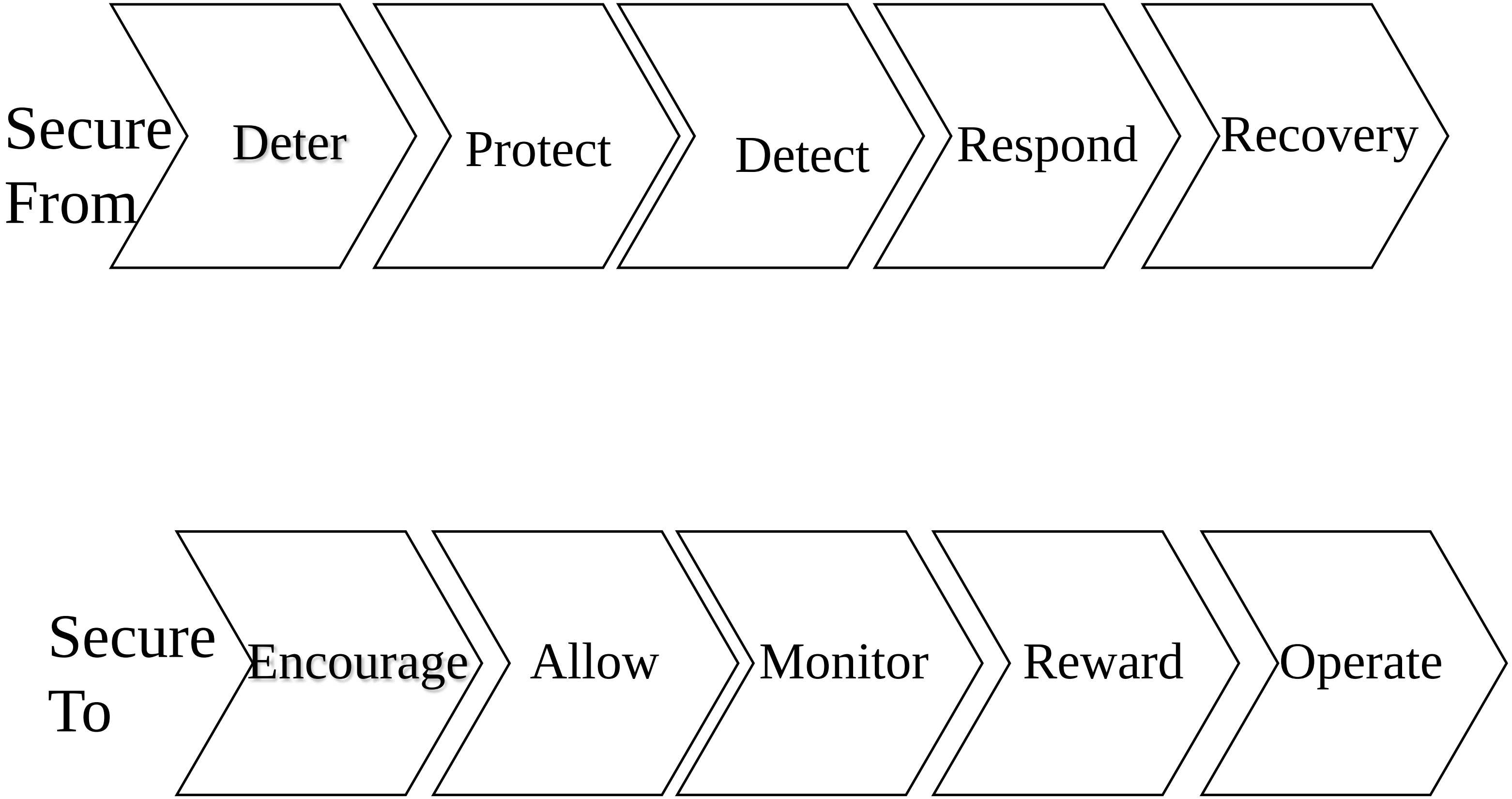
Access and connection

Marketing

OK OK NOT OK OK OK

The interconnect group of industry participants that collectively create value for the end user.If technologies or services are to succeed they must deliver financial or operational value at every stage of the chain. For any technology or service to be adopted, each element on the chain must add value for the next element.The strategic Implications of Computing and the Internet on Wireless: The Competitive Blur Through 2008, Herschel Shtick Associates.)

Theoretical
Insecurity and Security Value Chains
(Secure from Secure to)



Secure From

Deter

Protect

Detect

Respond

Recovery

Secure To

Encourage

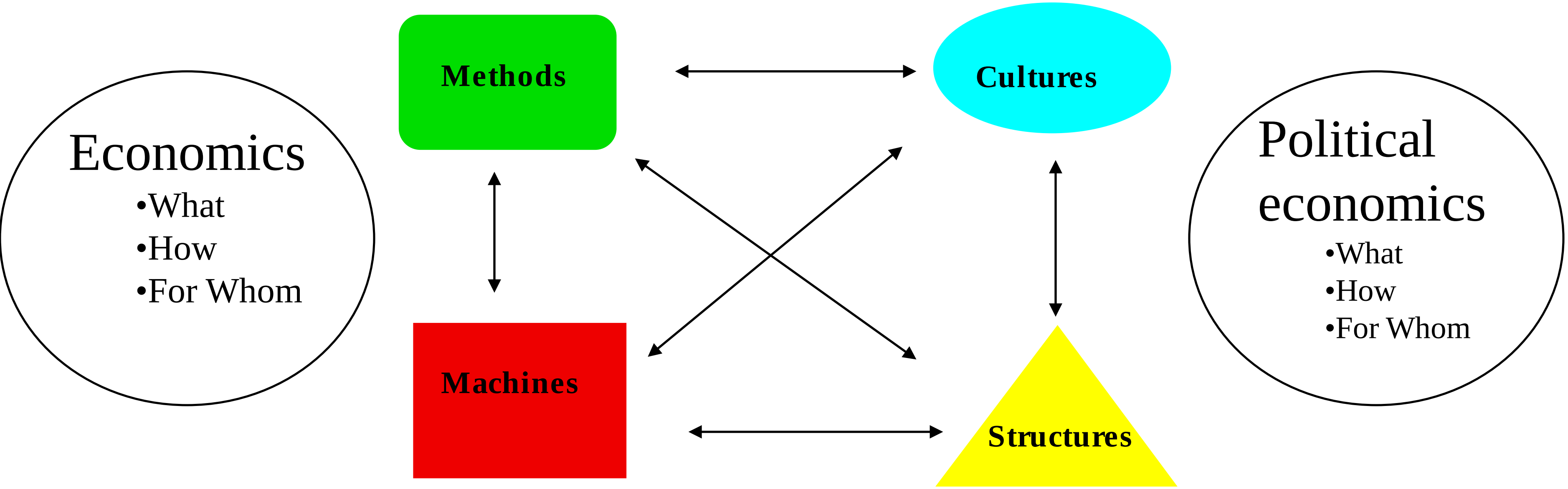
Allow

Monitor

Reward

Operate

The Model of the Century.-)
Common identifiable and observable characteristics of any human organization!
http://dsv.su.se/en/seclab/pages/pdf-files/94-004.pdf



Economics
- What
- How
- For Whom

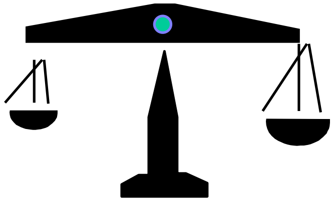
Methods

Cultures

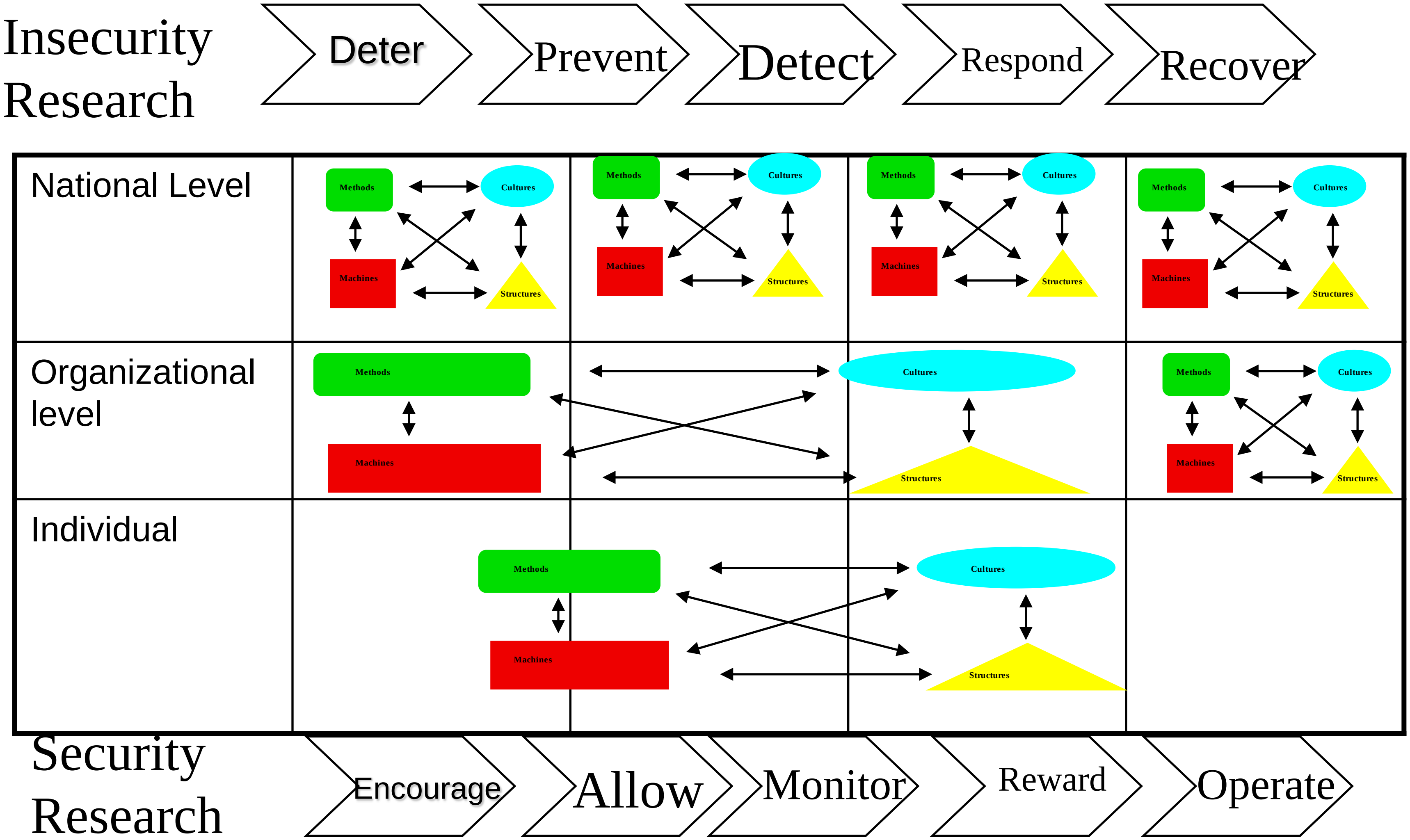
Machines

Structures

Political economics
- What
- How
- For Whom



Different Levels
Differnt Social tehcnial System in the Chain



Insecurity Research

Deter

Prevent

Detect

Respond

Recover

National Level

Organizational level

Individual

Security Research

Encourage

Allow

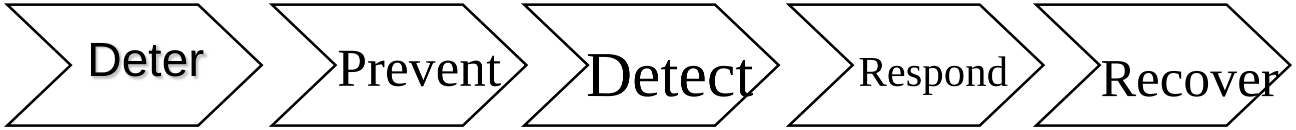
Monitor

Reward

Operate

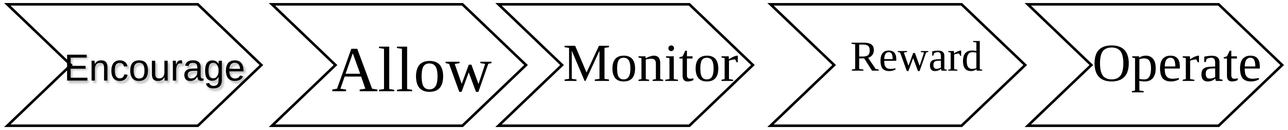
THE Matrix
Theoretical model of Insecurity and Security and Risk Research

Insecurity Research

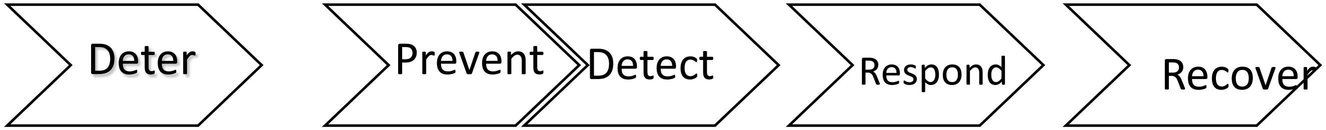


Social	Knowledge Tools Methods etc	Knowledge Tools Methods etc	Knowledge Tools Methods etc	Knowledge Tools Methods etc
Economics	Knowledge Tools Methods etc	Knowledge Tools Methods etc	Knowledge Tools Methods etc	Knowledge Tools Methods etc
Technical	Knowledge Tools Methods etc	Knowledge Tools Methods etc	Knowledge Tools Methods etc	Knowledge Tools Methods etc

Security Research



Cyber Security Private Public For Norway
Responsibility , Authority, and Competence Matrix
Sector {x, y,z…..}


Deter

Prevent

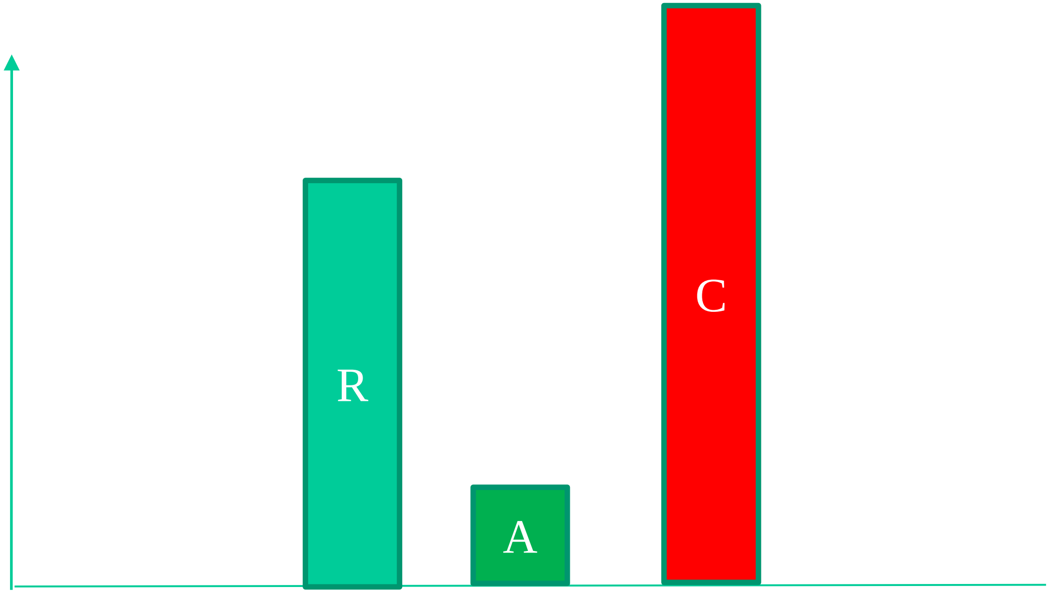
Detect

Respond

Recover

Public				
Public/Private				
Private				

RAC Model
Responsibilities, Authority, Competence



CAR Model Canadian Army Responsibilities, Authority, Competence

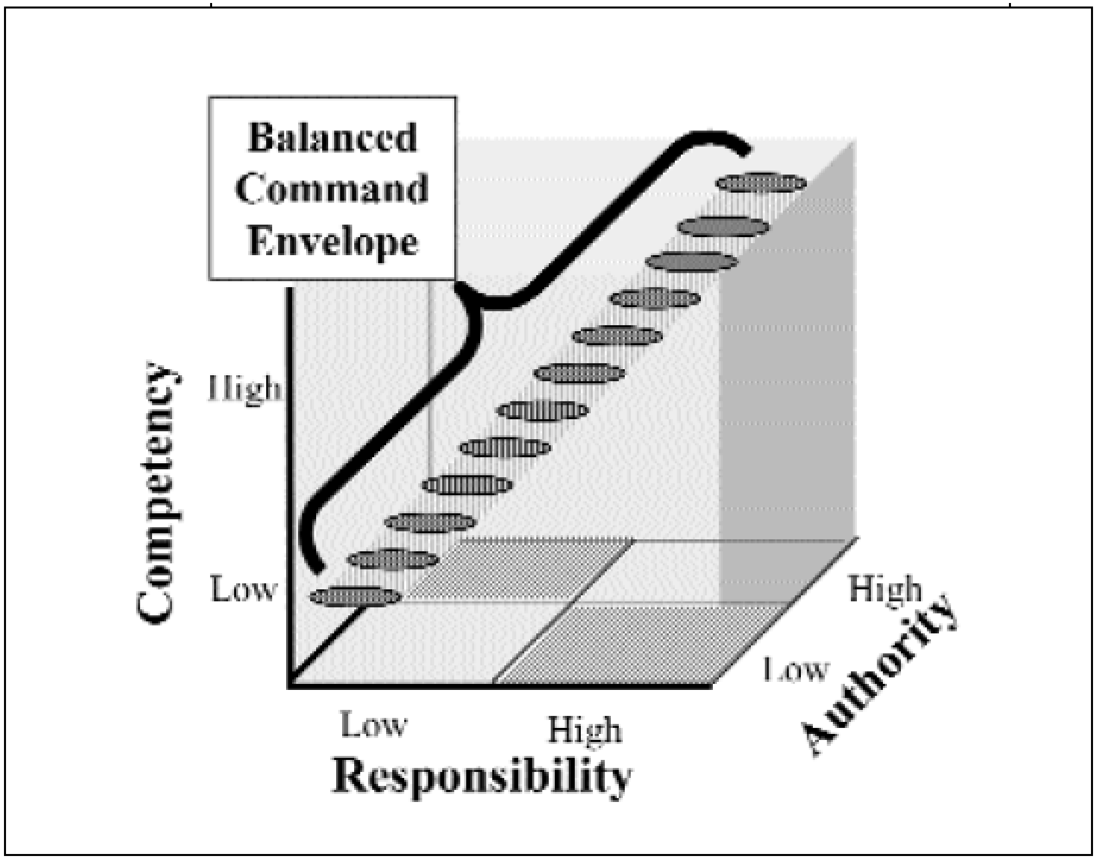
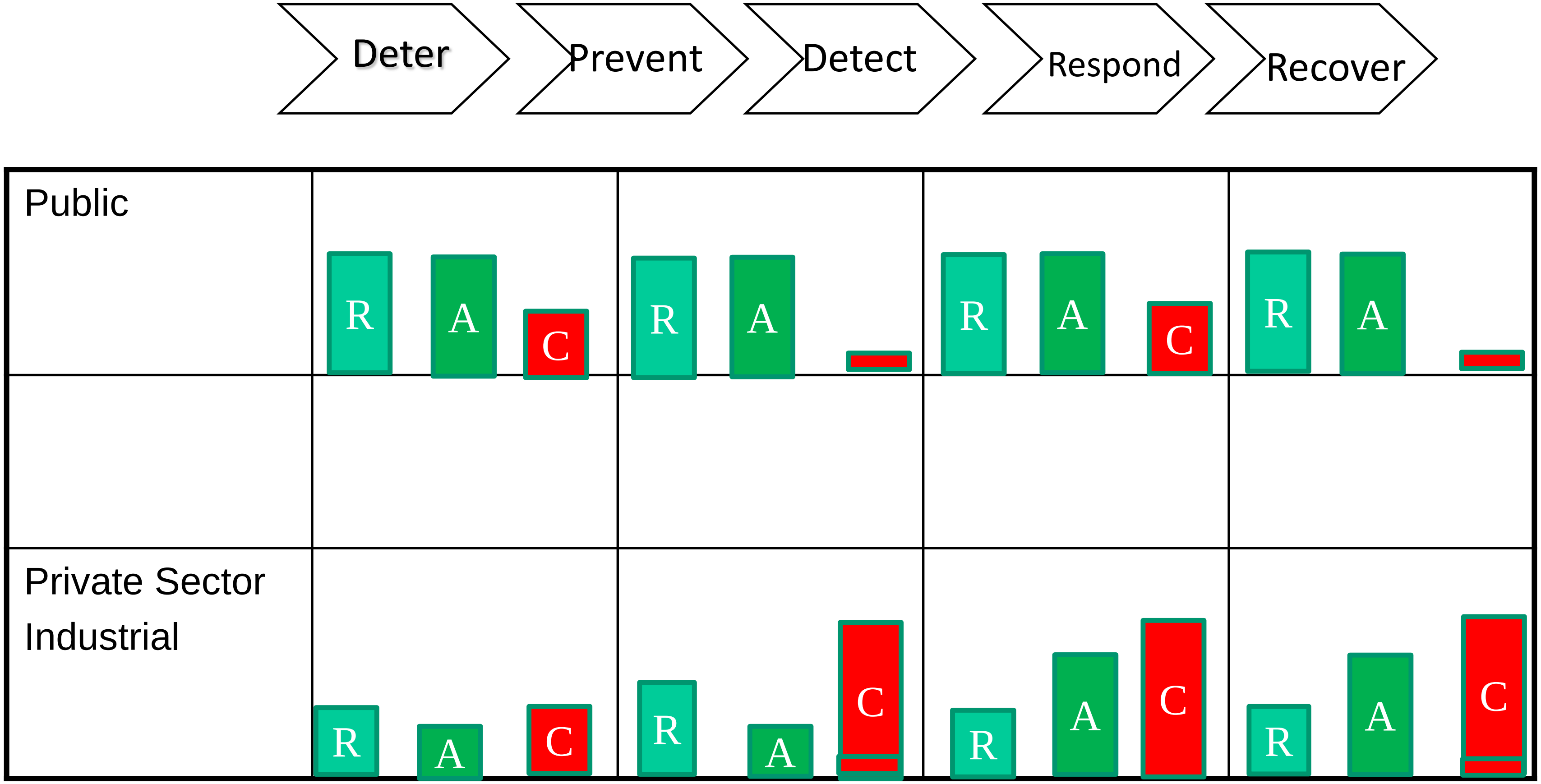


Figure 3 – The Balanced Command Envelope.

Soldiers of 'A' Squadron, The Royal Canadian Dragoons, get a briefing from their patrol commander at an observation post in Macedonia, September 2001.

Cyber Security Private Public For a Country
Responsibility , Authority, and Competence Matrix
Sector {x, y,z…..}



Deter

Prevent

Detect

Respond

Recover

Public

Private Sector

Industrial

Three Step Process

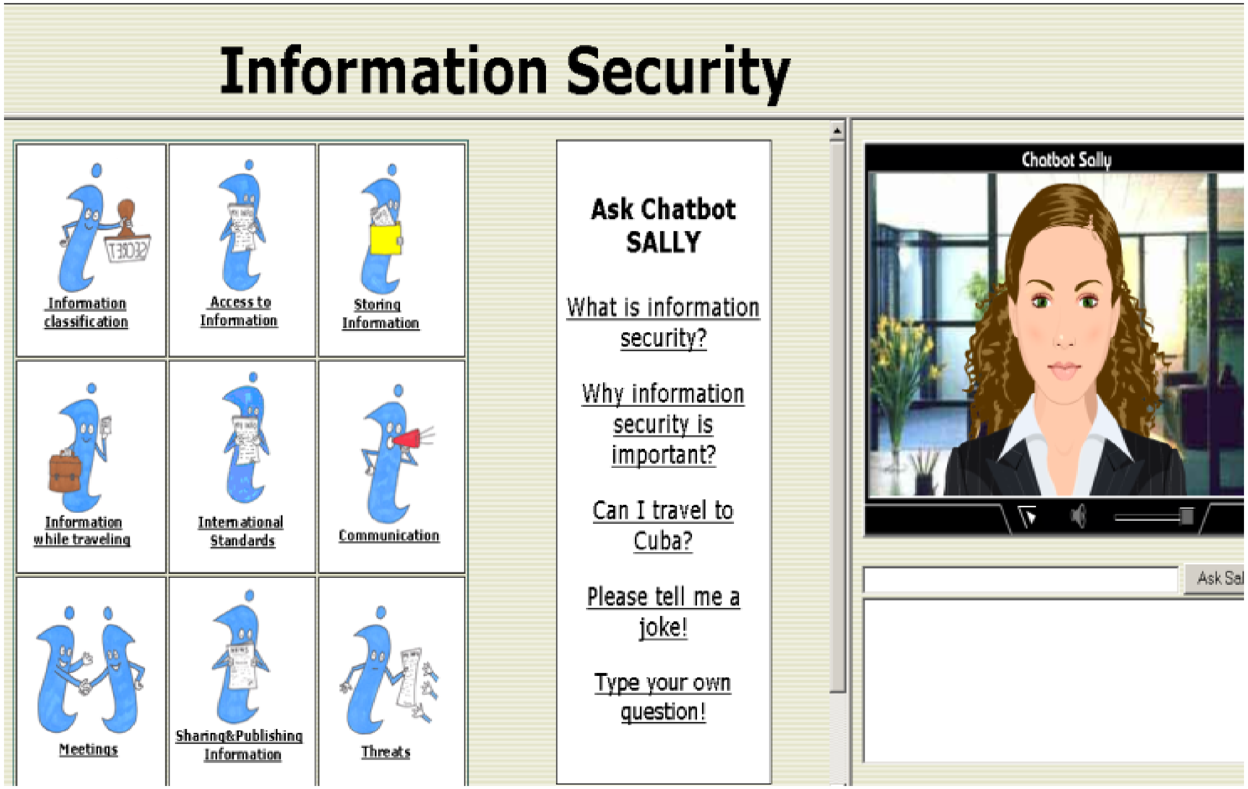
- Identify where the weak leaks are in the current concrete and abstract security value chain for different countries
- Establish responsibility , authority and competence charts for these links
- Identify short term and long term strategy for strength the competence in the weakest links by “Massive Online Open Courses” in Cyber Security for developing countries- i.e HIPing security eductation as we did in industry.

HIPing

Hyper

Interactive

Presenter



Information Security

Ask Chatbot SALLY

What is information security?

Why information security is important?

Can I travel to Cuba?

Please tell me a joke!

Type your own question!

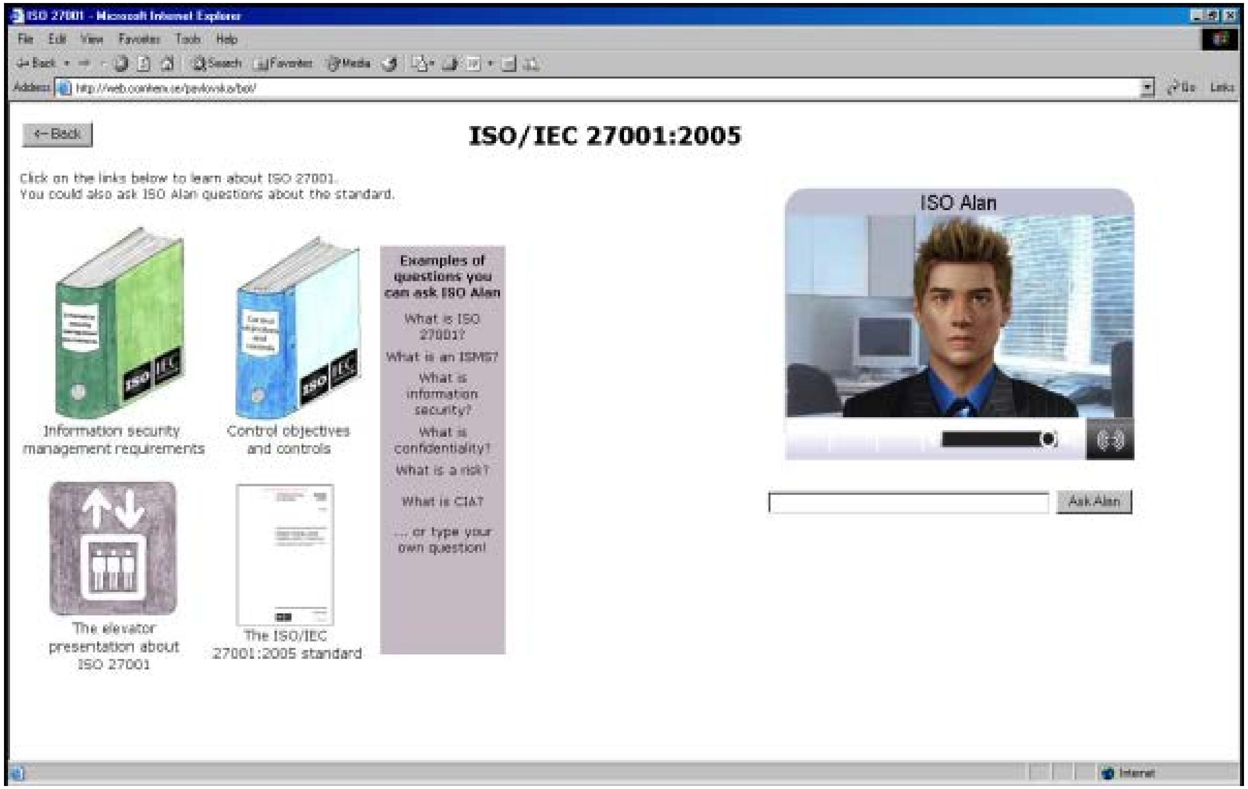
Ericsson Global Services 2008

HIPing

Hyper

Interactive

Presenter


ISO 27001 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://web.comhem.se/pavlovska/bot/
Go Links
← Back
ISO Alan
Ask Alan
Internet

ISO/IEC 27001:2005

Click on the links below to learn about ISO 27001.
You could also ask ISO Alan questions about the standard.

Information security management requirements

Control objectives and controls

The elevator presentation about ISO 27001

The ISO/IEC 27001:2005 standard

Examples of questions you can ask ISO Alan

What is ISO 27001?

What is an ISMS?

What is information security?

What is confidentiality?

What is a risk?

What is CIA?

... or type your own question!

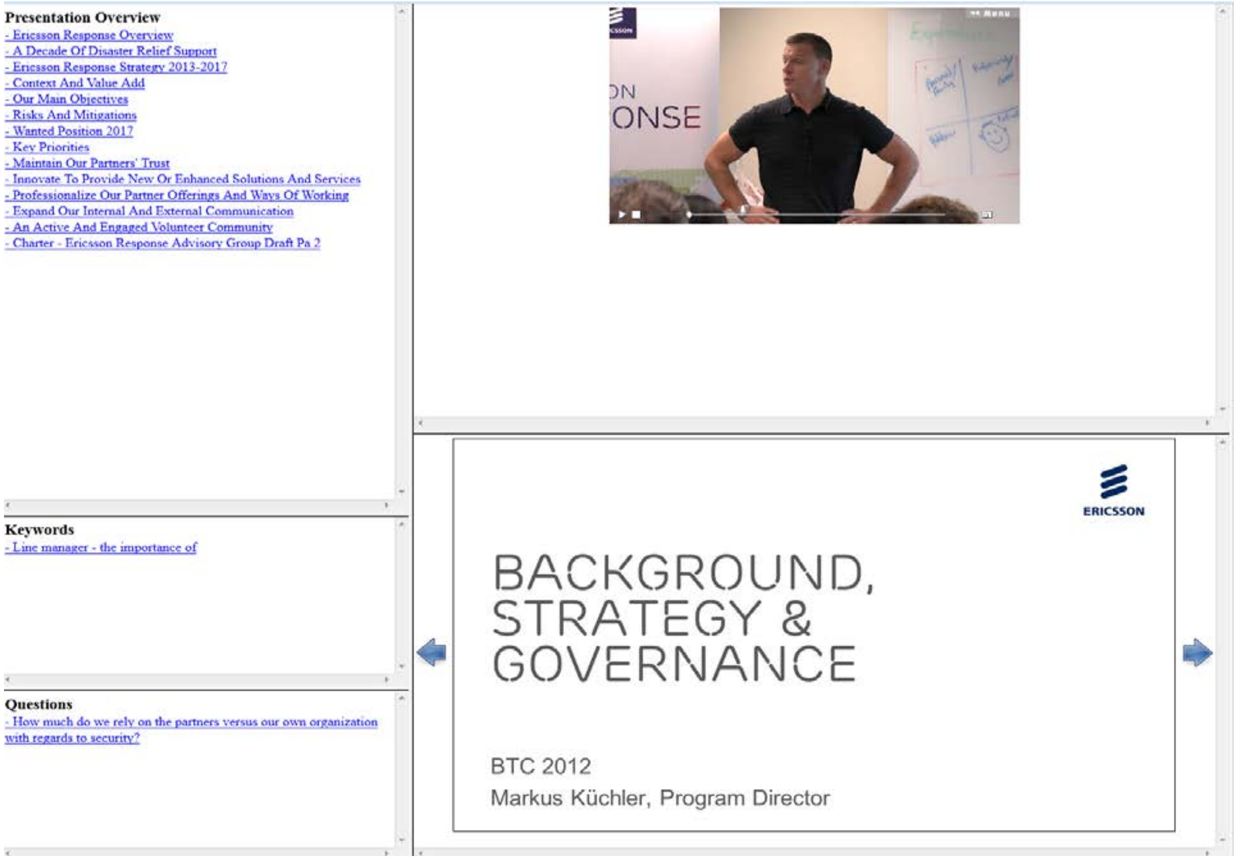
Ericsson Global Services 2008

HIPing

Hyper

Interactive

Presenter



Presentation Overview

- Ericsson Response Overview
- A Decade Of Disaster Relief Support
- Ericsson Response Strategy 2013-2017
- Context And Value Add
- Our Main Objectives
- Risks And Mitigations
- Wanted Position 2017
- Key Priorities
- Maintain Our Partners' Trust
- Innovate To Provide New Or Enhanced Solutions And Services
- Professionalize Our Partner Offerings And Ways Of Working
- Expand Our Internal And External Communication
- An Active And Engaged Volunteer Community
- Charter - Ericsson Response Advisory Group Draft Pa 2

Keywords

- Line manager - the importance of

Questions

- How much do we rely on the partners versus our own organization with regards to security?

ERICSSON

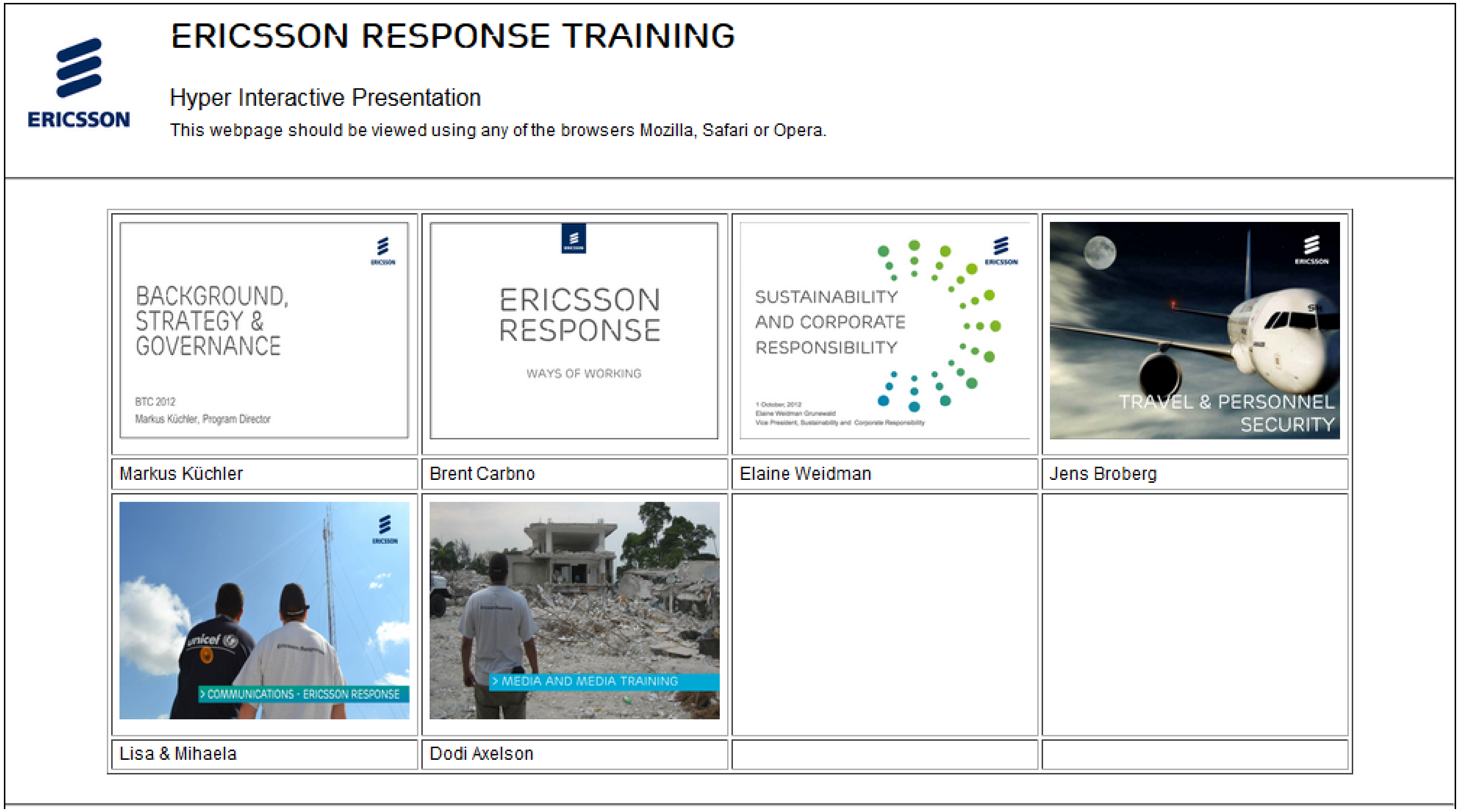
BACKGROUND,
STRATEGY &
GOVERNANCE

BTC 2012

Markus Küchler, Program Director

Ericsson Response 2012

http://alishariq.net/alishariq/ERT/



ERICSSON RESPONSE TRAINING

Hyper Interactive Presentation

This webpage should be viewed using any of the browsers Mozilla, Safari or Opera.

Markus Küchler	Brent Carbno	Elaine Weidman	Jens Broberg
Lisa & Mihaela	Dodi Axelson		

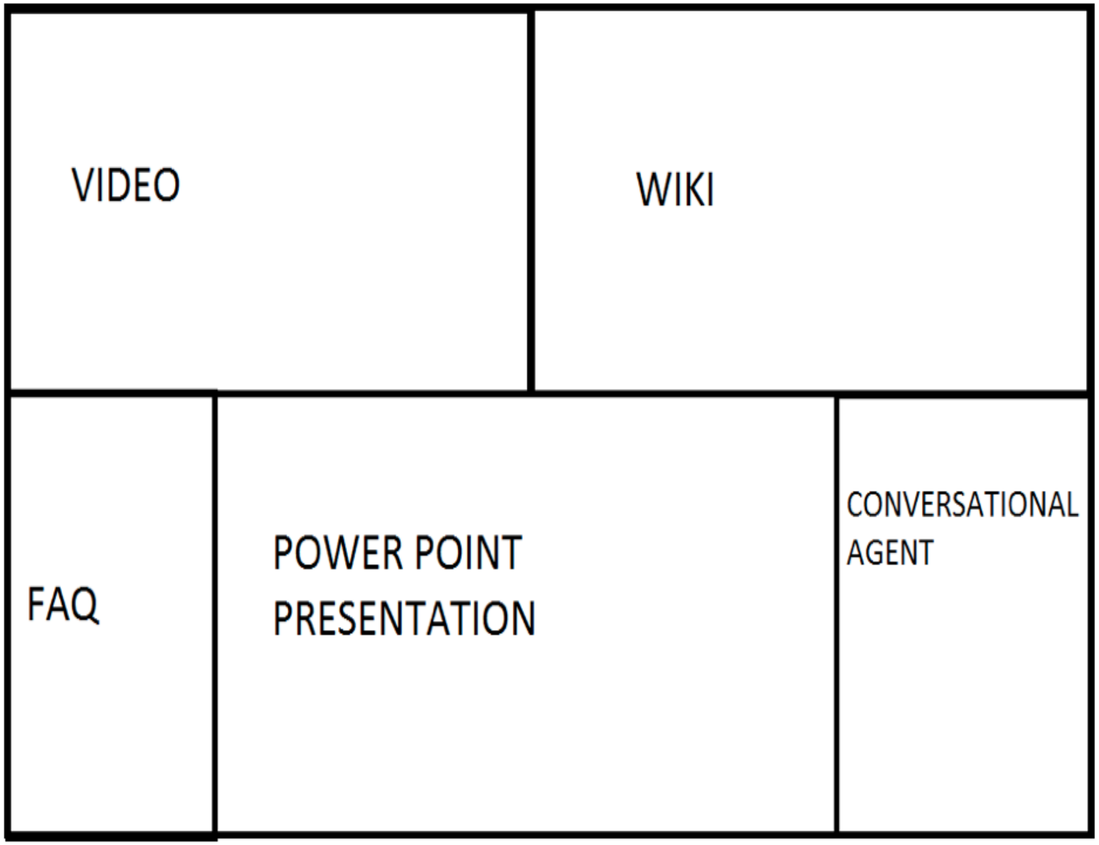
ERICSSON
BACKGROUND, STRATEGY & GOVERNANCE
BTC 2012
Markus Küchler, Program Director
ERICSSON RESPONSE
WAYS OF WORKING
SUSTAINABILITY AND CORPORATE RESPONSIBILITY
1 October, 2012
Elaine Weidman Grunewald
Vice President, Sustainability and Corporate Responsibility
TRAVEL & PERSONNEL SECURITY
> COMMUNICATIONS - ERICSSON RESPONSE
> MEDIA AND MEDIA TRAINING

HIPing

Hyper

Interactive

Presenter



VIDEO

WIKI

FAQ

POWER POINT PRESENTATION

CONVERSATIONAL AGENT

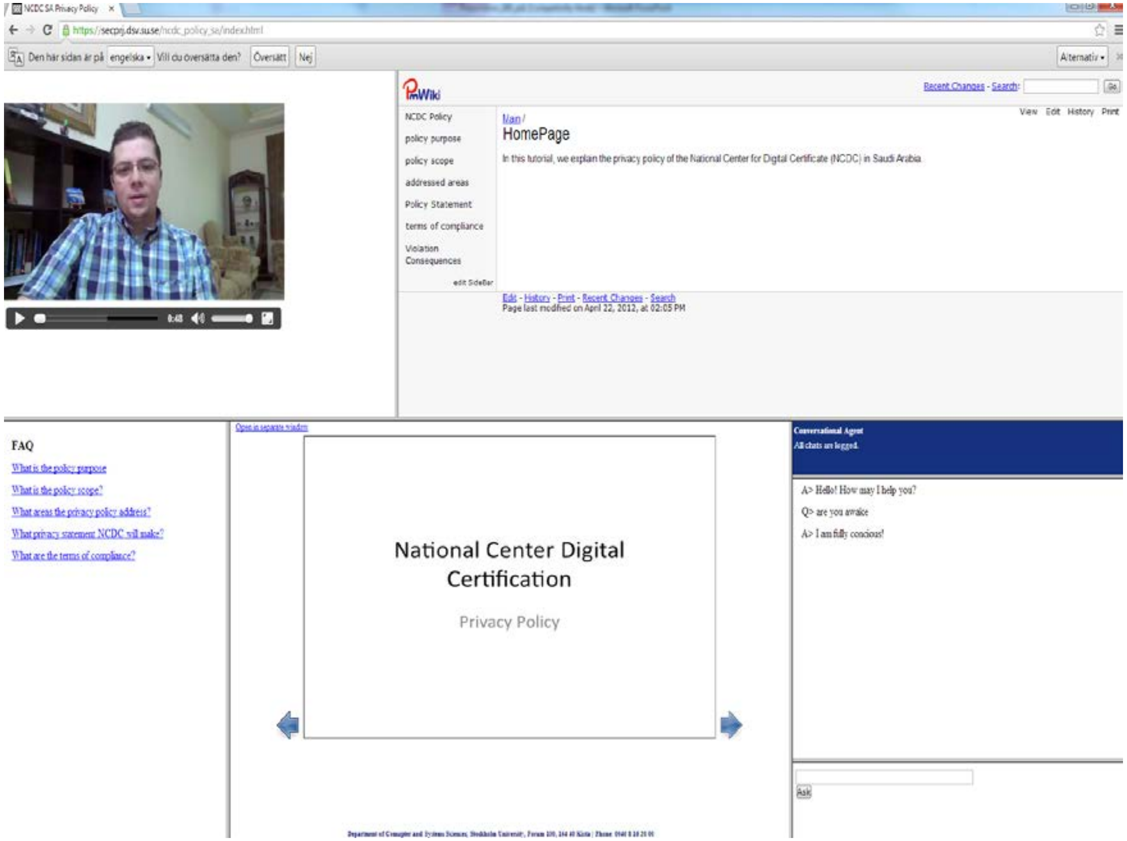
2012

HIPing

Hyper

Interactive

Presenter



NCDC SA Privacy Policy

https://secprj.dsv.su.se/ncdc_policy_sa/index.html

Den här sidan är på engelska ▾ Vill du översätta den? Översätt Nej Alternativ ▾

PmWiki

Recent Changes - Search: Go

View Edit History Print

- NCDC Policy
- policy purpose
- policy scope
- addressed areas
- Policy Statement
- terms of compliance
- Violation Consequences

edit SideBar

Main /

HomePage

In this tutorial, we explain the privacy policy of the National Center for Digital Certificate (NCDC) in Saudi Arabia

Edit - History - Print - Recent Changes - Search

Page last modified on April 22, 2012, at 02:05 PM

FAQ

- What is the policy purpose
- What is the policy scope?
- What areas the privacy policy address?
- What privacy statement NCDC will make?
- What are the terms of compliance?

Open in separate window

National Center Digital Certification

Privacy Policy

Department of Computer and Systems Sciences, Stockholm University, Forum 100, 164 40 Kista | Phone [illegible]

Conversational Agent

All chats are logged.

A> Hello! How may I help you?

Q> are you awake

A> I am fully concious!

Ask

https://secprj.dsv.su.se/ncdc_policy_sa/index.html

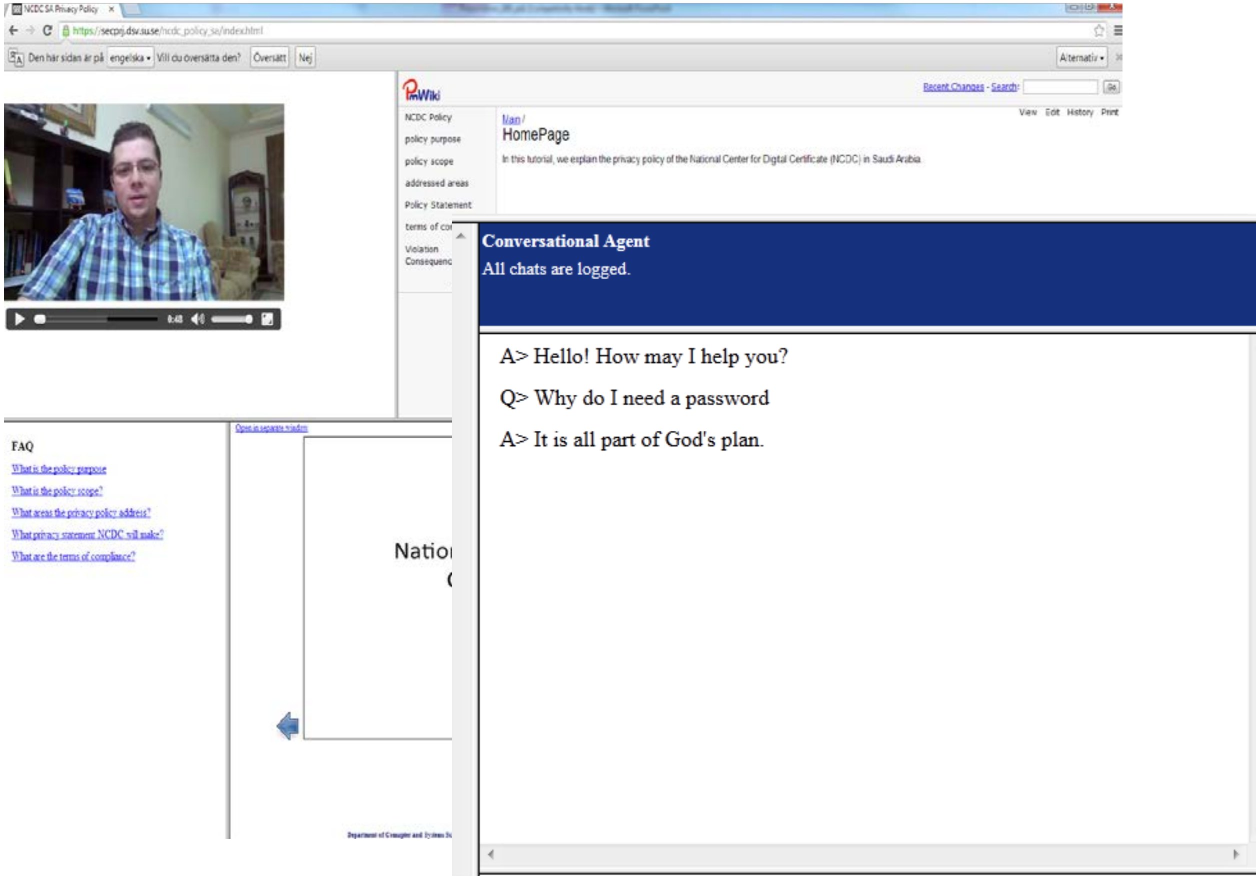
HIPing Privacy Saudi Arabia 2012

HIPing

Hyper

Interactive

Presenter



Main /

HomePage

In this tutorial, we explain the privacy policy of the National Center for Digital Certificate (NCDC) in Saudi Arabia

Conversational Agent

All chats are logged.

A> Hello! How may I help you?

Q> Why do I need a password

A> It is all part of God's plan.

FAQ

What is the policy purpose

What is the policy scope?

What areas the privacy policy address?

What privacy statement NCDC will make?

What are the terms of compliance?

https://secprj.dsv.su.se/ncdc_policy_sa/index.html

HIPing

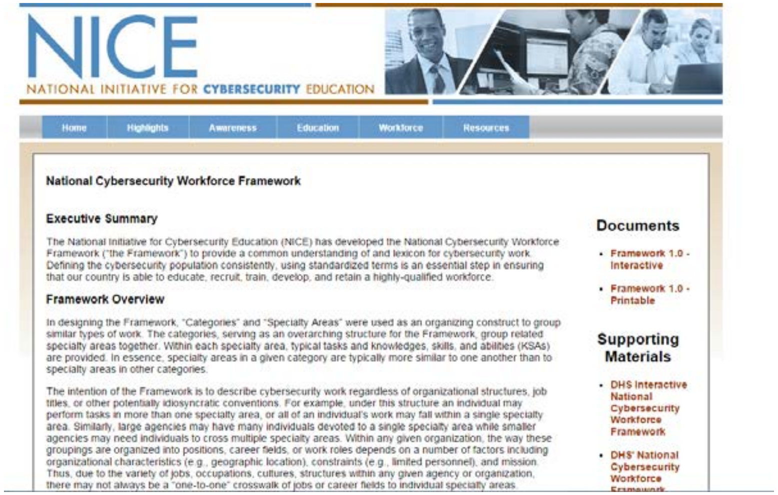
The GAP

Security ↔ Media ↔ Citizen

Management Employee

Government Agency Mind (s)

USA



National Cybersecurity Workforce Framework

Executive Summary

The National Initiative for Cybersecurity Education (NICE) has developed the National Cybersecurity Workforce Framework ("the Framework") to provide a common understanding of and lexicon for cybersecurity work. Defining the cybersecurity population consistently, using standardized terms is an essential step in ensuring that our country is able to educate, recruit, train, develop, and retain a highly-qualified workforce.

Framework Overview

In designing the Framework, "Categories" and "Specialty Areas" were used as an organizing construct to group similar types of work. The categories, serving as an overarching structure for the Framework, group related specialty areas together. Within each specialty area, typical tasks and knowledges, skills, and abilities (KSAs) are provided. In essence, specialty areas in a given category are typically more similar to one another than to specialty areas in other categories.

The intention of the Framework is to describe cybersecurity work regardless of organizational structures, job titles, or other potentially idiosyncratic conventions. For example, under this structure an individual may perform tasks in more than one specialty area, or all of an individual's work may fall within a single specialty area. Similarly, large agencies may have many individuals devoted to a single specialty area while smaller agencies may need individuals to cross multiple specialty areas. Within any given organization, the way these groupings are organized into positions, career fields, or work roles depends on a number of factors including organizational characteristics (e.g., geographic location), constraints (e.g., limited personnel), and mission. Thus, due to the variety of jobs, occupations, cultures, structures within any given agency or organization, there may not always be a "one-to-one" crosswalk of jobs or career fields to individual specialty areas.

Documents

- Framework 1.0 - Interactive
- Framework 1.0 - Printable

Supporting Materials

- DHS Interactive National Cybersecurity Workforce Framework
- DHS' National Cybersecurity Workforce Framework

The GAP

Security ↔ Media ↔ Citizen

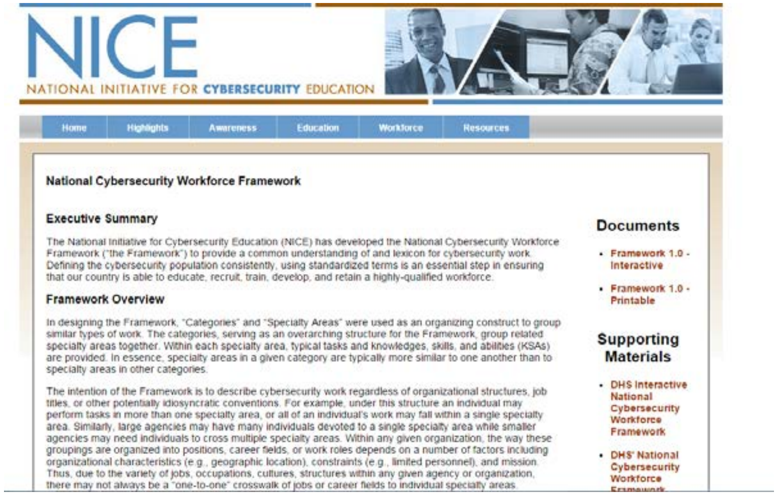
Management

Government Agency

Employee

Mind (s)

USA



National Cybersecurity Workforce Framework

Executive Summary

The National Initiative for Cybersecurity Education (NICE) has developed the National Cybersecurity Workforce Framework ("the Framework") to provide a common understanding of and lexicon for cybersecurity work. Defining the cybersecurity population consistently, using standardized terms is an essential step in ensuring that our country is able to educate, recruit, train, develop, and retain a highly-qualified workforce.

Framework Overview

In designing the Framework, "Categories" and "Specialty Areas" were used as an organizing construct to group similar types of work. The categories, serving as an overarching structure for the Framework, group related specialty areas together. Within each specialty area, typical tasks and knowledges, skills, and abilities (KSAs) are provided. In essence, specialty areas in a given category are typically more similar to one another than to specialty areas in other categories.

The intention of the Framework is to describe cybersecurity work regardless of organizational structures, job titles, or other potentially idiosyncratic conventions. For example, under this structure an individual may perform tasks in more than one specialty area, or all of an individual's work may fall within a single specialty area. Similarly, large agencies may have many individuals devoted to a single specialty area while smaller agencies may need individuals to cross multiple specialty areas. Within any given organization, the way these groupings are organized into positions, career fields, or work roles depends on a number of factors including organizational characteristics (e.g., geographic location), constraints (e.g., limited personnel), and mission. Thus, due to the variety of jobs, occupations, cultures, structures within any given agency or organization, there may not always be a "one-to-one" crosswalk of jobs or career fields to individual specialty areas.

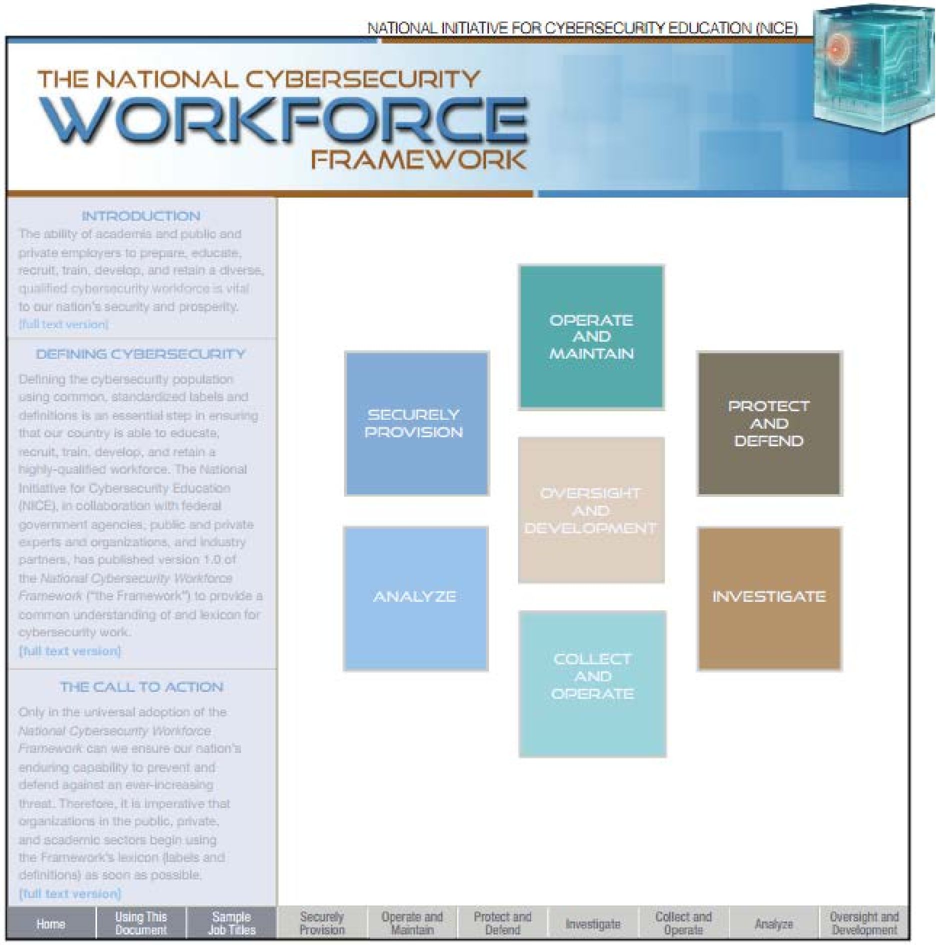
Documents

- Framework 1.0 - Interactive
- Framework 1.0 - Printable

Supporting Materials

- DHS Interactive National Cybersecurity Workforce Framework
- DHS' National Cybersecurity Workforce Framework

Online Knowledge
Platform for online problmes!


NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)
THE NATIONAL CYBERSECURITY
WORKFORCE
FRAMEWORK

INTRODUCTION

The ability of academia and public and private employers to prepare, educate, recruit, train, develop, and retain a diverse, qualified cybersecurity workforce is vital to our nation's security and prosperity.
[full text version]

DEFINING CYBERSECURITY

Defining the cybersecurity population using common, standardized labels and definitions is an essential step in ensuring that our country is able to educate, recruit, train, develop, and retain a highly-qualified workforce. The National Initiative for Cybersecurity Education (NICE), in collaboration with federal government agencies, public and private experts and organizations, and industry partners, has published version 1.0 of the *National Cybersecurity Workforce Framework* ("the Framework") to provide a common understanding of and lexicon for cybersecurity work.
[full text version]

THE CALL TO ACTION

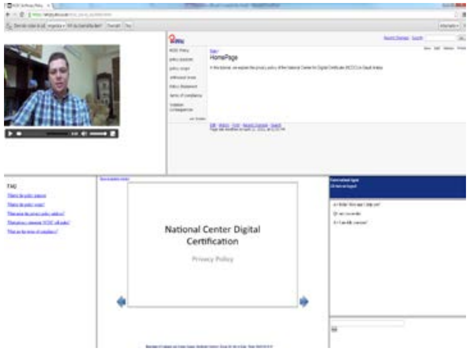
Only in the universal adoption of the *National Cybersecurity Workforce Framework* can we ensure our nation's enduring capability to prevent and defend against an ever-increasing threat. Therefore, it is imperative that organizations in the public, private, and academic sectors begin using the Framework's lexicon (labels and definitions) as soon as possible.
[full text version]

http://csrc.nist.gov/nice/framework/national_cybersecurity_workforce_framework_03_2013_version1_0_interactive.pdf

HIPing The GAP

Security
Management
ITU-T

↔



HomePage

FAQ

National Center Digital Certification

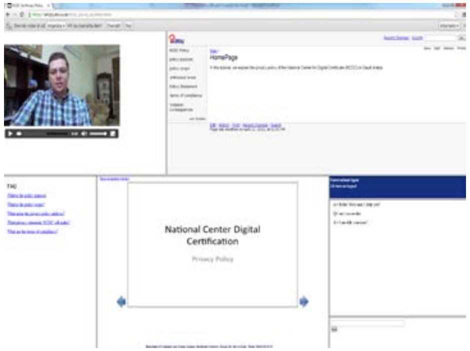
Privacy Policy

↔

Citizen
Employee
Mind (s)

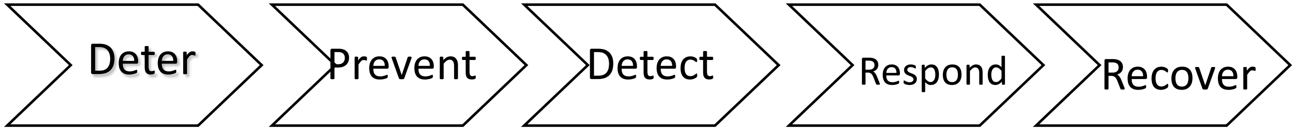
HIPing The GAP

Security Management ⟷



⟷ Citizen Employee Mind (s)

HIP is a educational platform to establishing, and maintaining information security competence in the developing world at a reasonable cost!



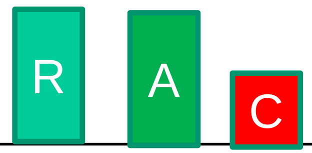
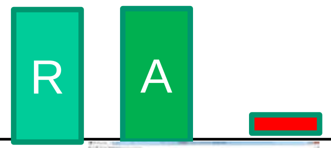
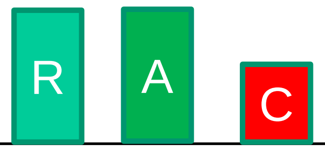
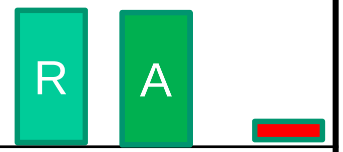
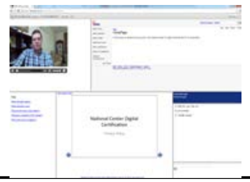
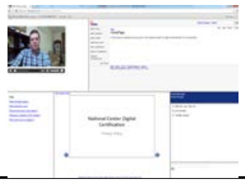
Deter

Prevent

Detect

Respond

Recover

Public				
Fill the gap With HIPed Mindes				
Private Sector Industrial