# SOCIAL ENGINEERING FRAMEWORK

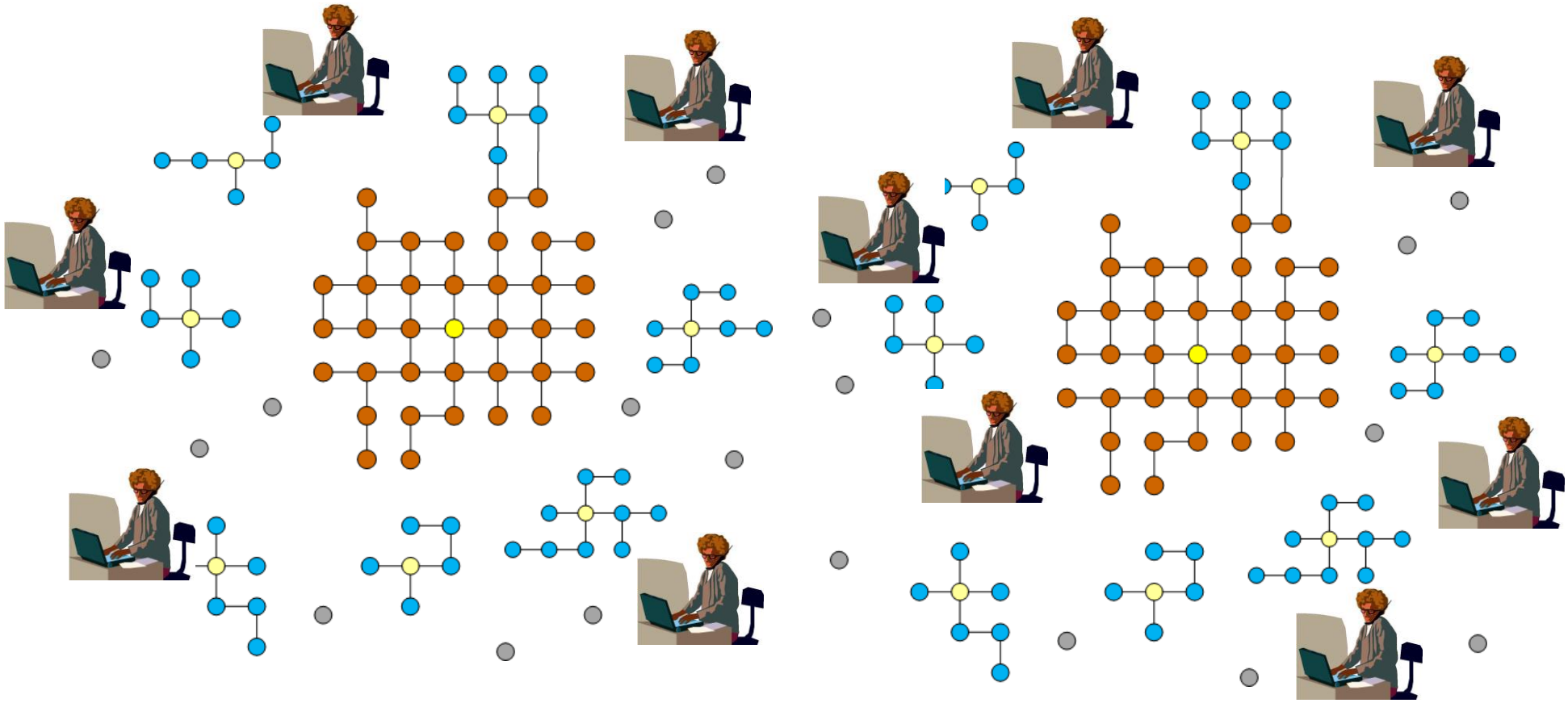
## SAFEGUARDING YOURSELF FROM SOCIAL ENGINEERING ATTACKS:

Understanding the Deception Strategy to Build Human Firewalls

**Prof. Richardus Eko Indrajit**

indrajit@alumni.harvard.edu
http://eko.id (+62) 818.925.926

# The Posture of Internet



# The Strength of a Chain

**"The STRENGTH of a CHAIN depends on the WEAKEST LINK"**

**WHAT and WHERE is the WEAKEST LINK**

**?**

# Human as the Weakest Link

- A lack of security awareness
- Education background
- Low technology literacy
- Positive thinking tendency
- Friends and family relationship
- Sharing and collaboration culture
- Trust society environment
- IT people and division dependence
- Paradigm on internet security
- Laziness in handling technical matters

# Ways to Exploit Human Vulnerabilities

- Offering help
- Asking for assistance
- Serving the customers
- Giving technical instructions
- Facilitating the works
- Delivering presents
- Sharing experience
- Promoting valuable products
- Informing emergency alert
- Installing software
- Abusing power/authority

# Social Engineering Definition

- Various techniques that are utilised to obtain information in order to bypass security system through the exploitation of human vulnerability
- Using human deception as means for information theft
- Malicious intent of cyber attackers attempting to illegally compromise an organisation's assets by using relationship with people
- The art of using persuasion and/or deception to gain access to information systems

# Challenges on Social Engineering

- So many variants in nature
- Embedded within human culture and behaviors
- Different from time to time
- Permutation of all possibilities
- High success rate of endeavors
- Difficult to mitigate
- Lack of research efforts

# Research Objectives

**1**

**Define the patterns on social engineering efforts**

**2**

**Find the strategy to mitigate the risks**

| KNOWLEDGE DOMAIN | | LITERATURE |
|---|---|---|
| **Definition of Social Engineering** | : | (Bezuidenhout et.al., 2010), (Hermansson et.al., 2005), (Huber, 2009), (Dolan, 2004), (Long, 2008), (Evans, 2009), (Foozy, 2011), (McClure, 2005) |
| **Reasons of Choosing Social Engineering** | : | (Grossklags et.al., 2009) |
| **Nature of Social Engineering Attacks** | : | (Grossklags et.al., 2009), (Mattord, 2006), (Granger, 2001), (Tomhave, 2007), (Hoeschele, 2006), (Thapar, 2007), (Murray, 2011), (Warren et.al., 2006), (Lineberry, 2007) |
| **Psychological Aspects of Deception** | : | (Hadnagy, 2011), (Hermansson et.al., 2005) |
| **Type of Social Engineers and the Motivations** | : | (Pfleeger, 2003), (Hadnagy, 2012) |
| **Categories of Social Engineering** | : | (Hermansson et. al., 2005), (Turner, 2005), (Redmon, 2006), (Thapar, 2007), (Prince, 2009), (Granger, 2001), (Foozy et.al., 2011) |
| **Stages of Social Engineering Efforts** | : | (Gartner, 2001), (Warren et.al., 2006), (Engebretson, 2013), (Singh, 2013) |
| **Tools for Social Engineering** | : | (Hadnagy, 2011) |
| **Mitigation Approach** | : | (Morgan, 2006), (Thapar, 2007), (Thompson, 2003), (Mulligan, 2011), (Allen, 2001) |
| **Discourses** | : | (Omote, 2008), (Duff, 2005), (Mulligan et.al., 2011), (Thompson, 2003) |

| DOMAIN | | SOCIAL ENGINEERING CASES |
|---|---|---|
| International | : | **The 419 Nigerian Scam, Dalai Lama Server, Dark Market, Mati Bite, Alcohol Impact, IT Division Support, Stanley Mark Rifkin, Overconfident CEO, Theme-Park Scandal, Hack the Hackers, AOL Tech Support, Surveillance Camera Peeking, Fake Fire Alarms, Computer Teacher, Lost in Space, ISP Services, Consultancy Services, Parking Ticket, Transfer Notification, Profile Update Confirmation, Push Mail, Breaking News, Alumnie Gathering, Warning System, and Sampling Product** |
| National | : | **ATM Support, Bye-Bye Culture, TV Show Passwords, Old CC Machine, Emergency Surgery, Prize Winning, Forget-Password Remembering, Maintenance Call, Cross Password Referral, Phony Email, Former Executive Pass, Wall Mart Logistic Contract, Y2K Probono Consultant, Virus Cleaning, Secretary Priviledge, Flash Disk Copying, Software Installation, Fake Website, Credit Card Call Center, Used-Papers for Sale, Device Installation Services, After Sales Services, Hot Spot Request, Post It, and Active Login Decoy** |

| | |
|---|---|
| **PARADIGM** | Inductive Approach |
| | Extraction on Characteristics/Properties/Behaviors |
| | Analysing for Grouping/Classification/Clustering |
| | Pareto Principles on Prioritisation |
| | Principles and Architecture on Mitigation |
| **TYPES** | Qualitative (Case Studies + Experience) and Quantitative (Survey) |
| **QUESTIONS** | What is SE paradigms? |
| | How many types of SE exist? |
| | How the SE attacks are being done? |
| | What are the critical success factors? |
| | How to prevent SE? |
| **PROPOSITIONS** | There are several approaches of deceptions |
| | There are pre-conditions that should be met for success |
| | Every attempts is unique yet methodological |
| | Mitigation risks can be deployed to minimise negative impacts |

## Definition of Social Engineering

| Which definition of social engineering that is most suitable to your understanding? | | |
|---|---|---|
| A | Various techniques that are utilized to obtain information in order to bypass security systems, through the exploitation of human vulnerability | 40% |
| B | The term for using human deception as means for information theft | 24% |
| C | The art of exploiting the weakest link of information security systems: the people who are using them | 12% |
| D | Malicious intent of cyber attackers attempting to ilegally compromise an organisation's assets by using relationships with people | 16% |
| E | Description of techniques using persuasion and/or deception to gain access to information systems | 4% |
| O | Others | 4% |

## Motive of Social Engineering

| What was the motive of social engineering you've experienced in the past? | | |
|---|---|---|
| A | Economic benefits | 40% |
| B | Political gain | 0% |
| C | Image spoiling | 8% |
| D | Personal satisfaction | 40% |
| O | Others | 12% |

## Nature of Social Engineering Attack

| How do you considered the nature of social engineering activity you've experienced? | | |
|---|---|---|
| A | Direct attack | 12% |
| B | Indirect attack (to get confidential information for a real attack) | 84% |
| C | Do not know | 4% |
| O | Others | 0% |

## Social Engineering Approach

| What approach that was used during the pre-attack session (rapport building)? | | |
|---|---|---|
| A | Offering help or support | 12% |
| B | Introducing ideas to participate | 24% |
| C | Pretending to be someone else to assist special task | 20% |
| D | Asking to do some technical/administration activity | 40% |
| O | Others | 4% |

## Tools for Social Engineering

| What media mean that was used during the pre-attack session? | | |
|---|---|---|
| A | Email | 32% |
| B | Phone | 4% |
| C | Sms | 8% |
| D | Chatting | 44% |
| E | Face-to-face | 8% |
| O | Others | 4% |

## Reason to Choose Social Engineering

| What media mean that was used during the pre-attack session? | | |
|---|---|---|
| A | Easy | 76% |
| B | Cheap | 56% |
| C | Fast | 32% |
| D | Effective | 44% |
| E | Efficient | 32% |
| O | Others | 0% |

## Ratio of Success on Social Engineering

| Do you consider the effort a success? | | |
|---|---|---|
| A | Yes | 60% |
| B | No | 0% |
| C | Partially yes/no | 40% |
| O | Others | 0% |

## Possibility of Preventing Social Engineering

| Do you think such an attack can be prevented? | | |
|---|---|---|
| A | Yes | 60% |
| B | No | 4% |
| C | Partially yes/no | 36% |
| O | Others | 0% |

## Preventive Effort on Social Engineering

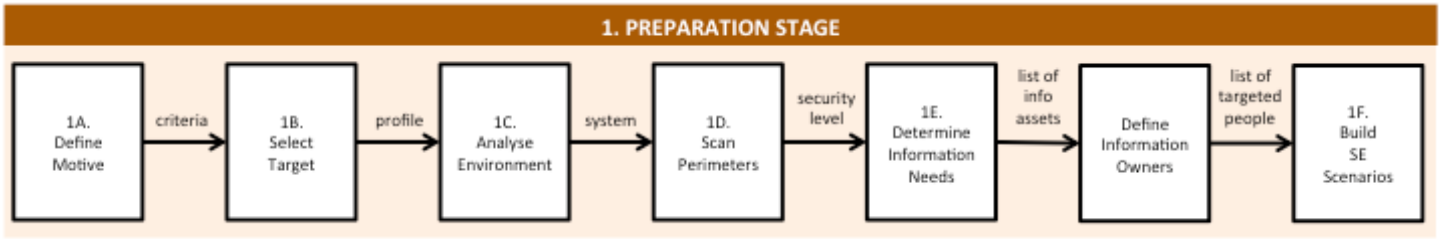
| What is the best way to prevent the social engineering attack? | | |
|---|---|---|
| A | Increase awareness | 68% |
| B | Increase education/socialisation | 20% |
| C | Increase literacy/knowledge/capability | 8% |
| O | Others | 4% |

## Mitigation Responsibility on Social Engineering

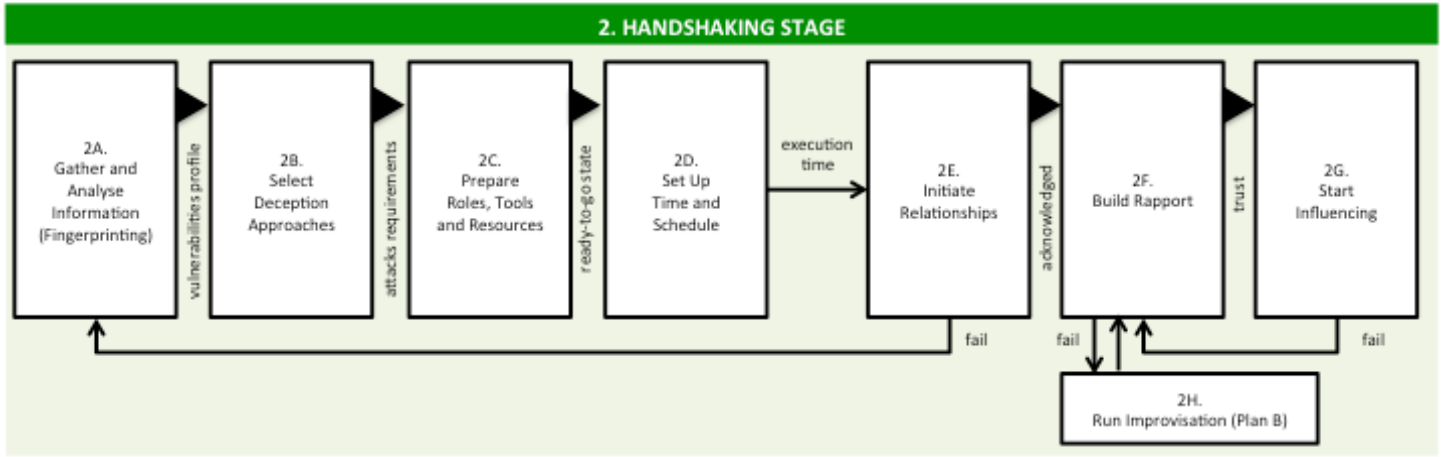
| What media mean that was used during the pre-attack session? | | |
|---|---|---|
| A | Users | 60% |
| B | Head of IT Division | 72% |
| C | Chief Executive Officer (Management) | 64% |
| D | Risk Management Unit | 80% |
| E | Legal Division | 64% |
| F | Call Center/Help Desk | 44% |
| O | Others | 8% |

The stage where criminals are trying to profile the victims

1



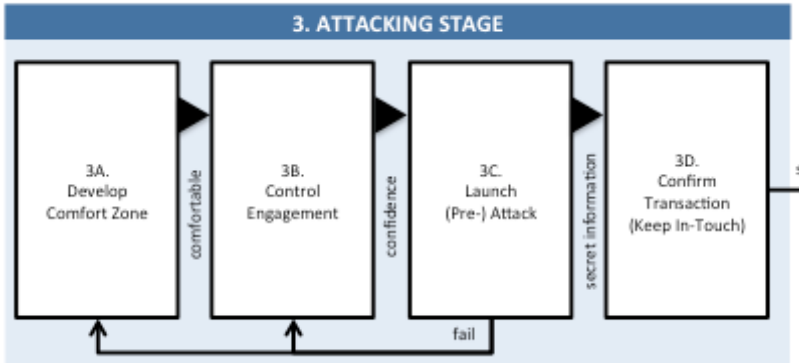

2

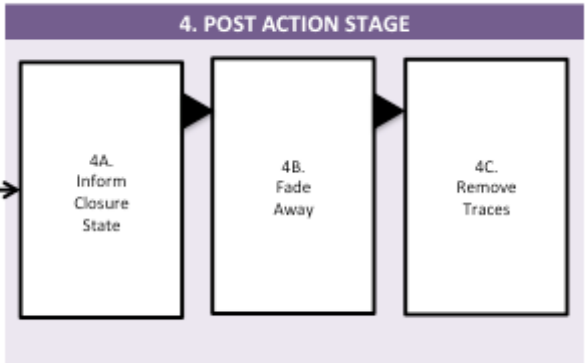



The stage where criminals are trying to build trust and strong relationship from the victims

The stage where criminals are exploiting the vulnerabilities

3




The stage where criminals are fading away and removing the trace

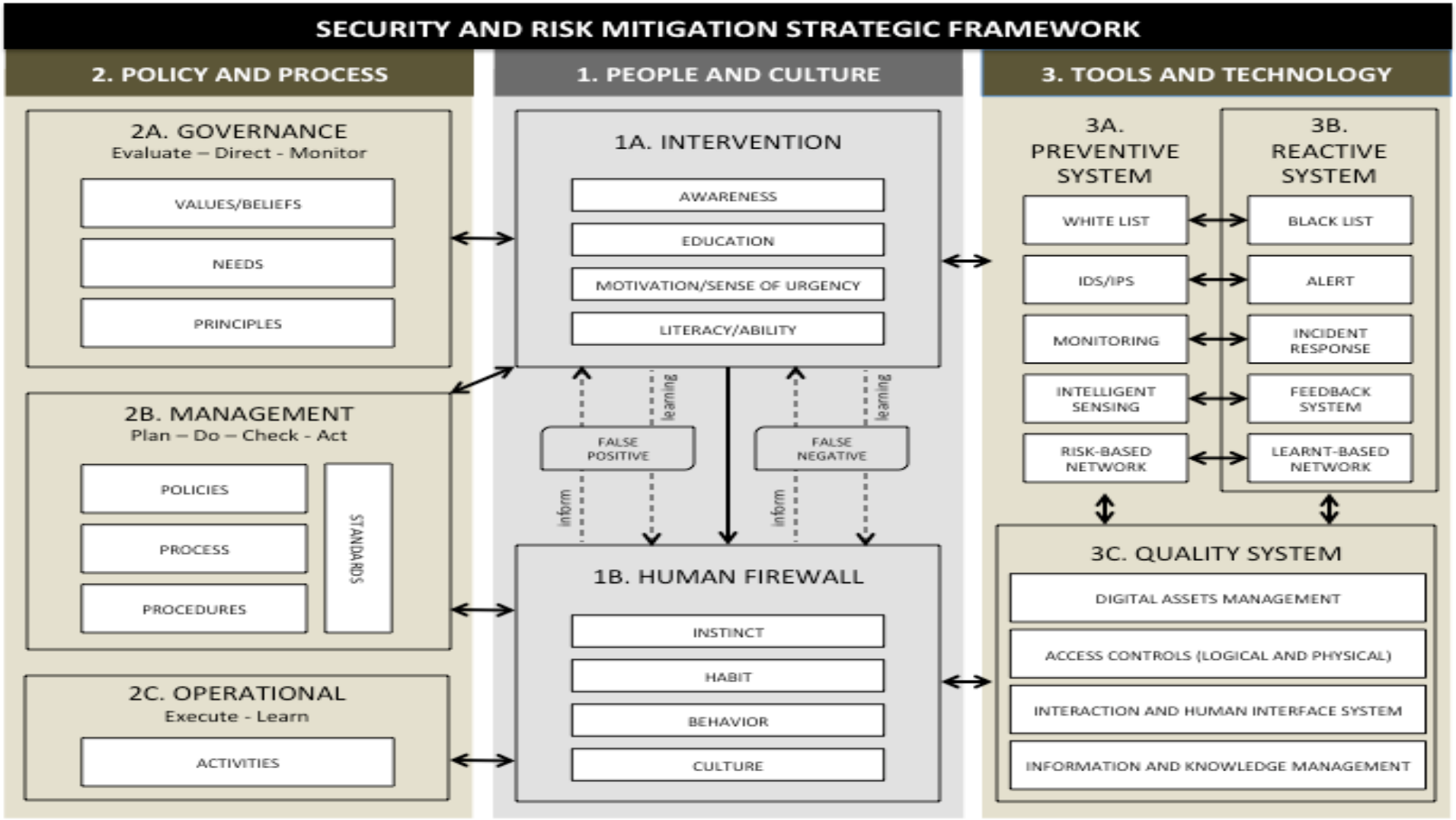
4

| 1. PREPARATION STAGE | | |
|---|---|---|
| **1A. Motive of Attacks** | : | Economic Benefits, Political Gain, Social Disorder, Image Spoiling, Cultural Disruption, Ideology/Value Challenge, Personal Satisfaction, War/Terror Creation |
| **1B. Target Selection** | : | Individual, Group, Organisation, Community, Public, Hybrid, Random |
| **1C. Environment Analysis** | : | Internal, External |
| **1D. Perimeter Scanning** | : | Physical, Logical |
| **1E. Information Requirements Analysis** | : | Technical, Non Technical |
| **1F. Asset Owners Determination** | : | Literate, Non/Low-Literate People |
| **1G.Scenario Development** | : | Pre-Attack, Attack Deployment, Post-Attack Action |

| 2. HANDSHAKING STAGE | | |
|---|---|---|
| **2A. Fingerprinting** | : | Profiling, Behavioral Analysis, Relationship Awareness, Social and Authority Status, Potential Vulnerabilities Posture |
| **2B. Deception Model** | : | Phishing, Pretexting, Baiting, Impersonating, Quid Pro Quo, Malware Planting, Physical Observation, Hoaxing, Elicitation, Reverse Social Engineering, Hybrid |
| **2C. Resource Preparation** | : | People, Process, Technology |
| **2D. Time and Schedule** | : | Prior to the D-Day, Deployment Time, Post Attack Period |
| **2E. Relationship Initiation** | : | Official Structure, Friends-and-Family, Supplier-Customer, Machine-Man, Personal Needs, Technical Requirements, Passive Roles |
| **2F. Rapport Building** | : | Empathy, Compliance, Solution, Protection, Scarcity, Comfort, Assistance |
| **2G. Influencing (Trust Building)** | : | Moral Duty, Help, Suggestion, Order, Persuasion, Fear Story, Help Desire, Warning, Intimidation, Ingratiation, Regulation |
| **2H. Improvisation Model** | : | Approach Alternate, Key Message Conveying |

| 3. ATTACKING STAGE | | |
|---|---|---|
| **3A. Comfort Zone Establishment** | : | Listening Well, Consistent Conversation, Value-Driven Topics |
| **3B. Engagement Control** | : | Command-Base Interaction, Encouragement |
| **3C. (Pre) Attacking Mode** | : | Direct/Explicit (Asset Disclosure), Indirect/Implicit (Leading Information) |
| **3D. Confirmation of Accomplishment** | : | Final Verification, Fake Governance |

| 4. POST ACTION STAGE | | |
|---|---|---|
| **4A. Closure** | : | Sympathy Message, Assistantship Offering |
| **4B. Fading Away** | : | Standby, Disappearance |
| **4C. Traces Removal** | : | Zero Path, Quick Audit |


SECURITY AND RISK MITIGATION STRATEGIC FRAMEWORK
2. POLICY AND PROCESS
1. PEOPLE AND CULTURE
3. TOOLS AND TECHNOLOGY
2A. GOVERNANCE
Evaluate – Direct - Monitor
VALUES/BELIEFS
NEEDS
PRINCIPLES
2B. MANAGEMENT
Plan – Do – Check - Act
POLICIES
PROCESS
PROCEDURES
STANDARDS
2C. OPERATIONAL
Execute - Learn
ACTIVITIES
1A. INTERVENTION
AWARENESS
EDUCATION
MOTIVATION/SENSE OF URGENCY
LITERACY/ABILITY
FALSE POSITIVE
FALSE NEGATIVE
aminate
inform
1B. HUMAN FIREWALL
INSTINCT
HABIT
BEHAVIOR
CULTURE
3A. PREVENTIVE SYSTEM
3B. REACTIVE SYSTEM
WHITE LIST
BLACK LIST
IDS/IPS
ALERT
MONITORING
INCIDENT RESPONSE
INTELLIGENT SENSING
FEEDBACK SYSTEM
RISK-BASED NETWORK
LEARNT-BASED NETWORK
3C. QUALITY SYSTEM
DIGITAL ASSETS MANAGEMENT
ACCESS CONTROLS (LOGICAL AND PHYSICAL)
INTERACTION AND HUMAN INTERFACE SYSTEM
INFORMATION AND KNOWLEDGE MANAGEMENT

# Conclusions and Recommendations

| | |
|---|---|
| **Conclusions** | There exist common methodology in SE |
| | There are four stages in deploying the attacks |
| | Holistic and systemic understanding is required |
| | Mitigation strategy should be well integrated |
| **Recommendations** | Every organisation is unique in vulnerabilities |
| | Map against the SE framework |
| | Examine the results for prioritisation |
| | Emphasise on related mitigation strategy |

# THANK YOU

## Questions and Answers

**Prof. Richardus Eko Indrajit**

indrajit@alumni.harvard.edu
http://eko.id (+62) 818.925.926