Yesterday
Today
Tomorrow

STEINBEIS-HOCHSCHULE
School of Management and Technology

Steinbeis
HOCHSCHULE

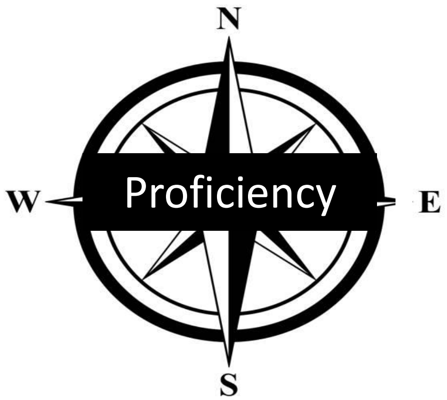
PROF. DR. JUAN CARLOS BARRERA

CYBER-SECURITY (BC6)

July 2020

Online Germany

Broadcasting from USA



Proficiency in Cybersecurity

Agenda:

1) Ethics and Decision-Making (A note on SETA)

2) Videos: Discussion & Reflection

3) Sixth Lab: Comprehensive Project & Practice

4) In Closing: Debriefing for Cases 01 – 02 – 03 – 04

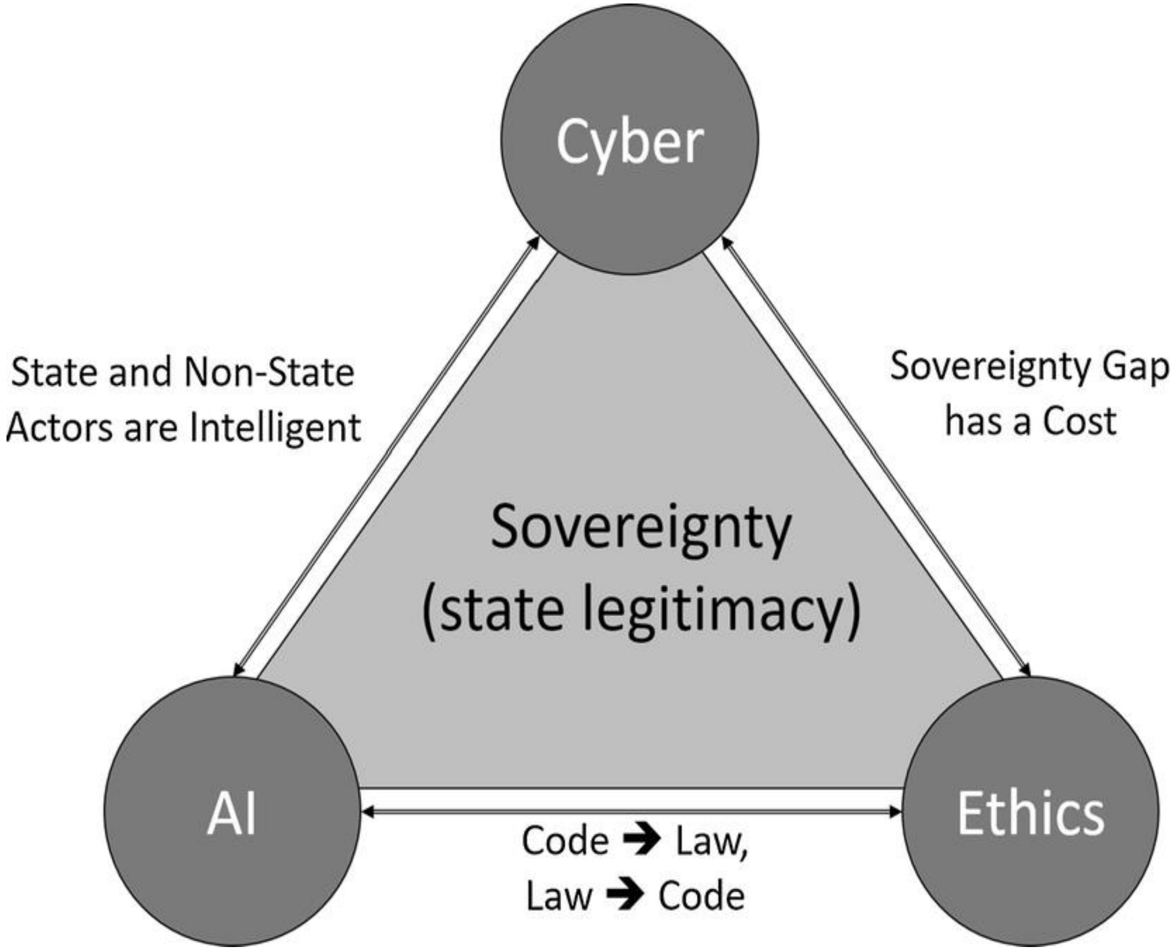
5) Exam

1) Ethics and Decision-Making

- Cyberspace if rife with temptations and ethical grey areas is because some of its intrinsic attributes:
- Cyberspace is a low-visibility environment – this leads to a level of anonymity and diminishes accountability
- Actors in cyberspace are often felt distant from the effects of their actions – this leads to the minimization of negative consequences
- Cyberspace is a relatively new domain – this leads to a frontier-mentality and a sense of impunity

Ethics (cont'd)

- Cybersecurity professionals must develop the clarity to know the difference between right and wrong and the character to make the right choice, even when nobody will probably ever know the difference.
- But how can one distinguish between right and wrong in the ethical grey areas of cyberspace?


Cyber
State and Non-State Actors are Intelligent
Sovereignty Gap has a Cost
Sovereignty (state legitimacy)
AI
Ethics
Code ➔ Law,
Law ➔ Code

Criteria for Evaluating Right and Wrong

Approach	Basis	Key Question
Utilitarian	Consequences	What are the anticipated benefits and harms to all of the affected parties?
Social Contract	Rights	Does this action violate the inherent rights of any of the involved parties?
Kantian	Motivations	Are any of the involved parties being treated as a means to an end?
Virtue Theory	Character	Does this action violate any moral virtues?

Removing Bias: The Veil of Ignorance

- The concept of a veil of ignorance is also a very helpful thought experiment for evaluating ethical grey areas
- One should make a judgment about right and wrong while pretending to not know to which group of affected parties he belongs to
- Is this applicable? How the veil of ignorance plays with the heuristics, biases, and bounded rationality?

- The concept of a veil of ignorance is also a very helpful thought experiment for evaluating ethical grey areas
- One should make a judgment about right and wrong while pretending to not know to which group of affected parties he belongs to
- Is this applicable? How the veil of ignorance plays with the heuristics, biases, and bounded rationality?

Example: Should Bob Tell or Not Tell?

Watch the video posted on Day 06

Conditions:

- There are only two parties that will be affected by Bob’s actions: himself and the president of the non-profit organization
- The actions Bob is contemplating are to tell or not to tell the president that he listened to the phone call

Exercise: Utilitarian Perspective

Utilitarian - What are the anticipated benefits and harms to all of the affected parties?

- By telling the president that he listened to the call, Bob would cause harm to himself (reprimand, lowered reputation, possible loss of wages) and harm to the president (humiliation, embarrassment, disappointment).
- The benefits of confessing seem marginal for both parties.
- Therefore, the harms of telling the president outweigh the benefits and Bob should NOT tell.

Exercise: Social Contract Perspective

Social contract - Does this action violate the inherent rights of any of the involved parties?

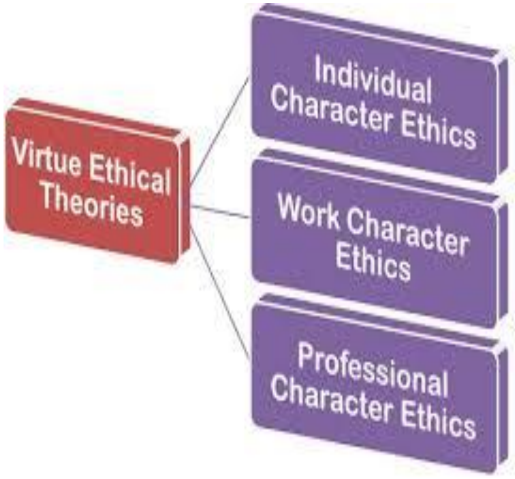
- Because the president is responsible for the organization, and he hired Bob to perform certain duties, he has a basic right to the information that Bob gleaned during the pen test.
- This includes, minimally, the right to know that VOIP calls are not encrypted – a highly relevant penetration test finding. It also (arguably) includes the right to know that Bob uncovered private information about the president
- Therefore, the president is entitled to the information and Bob should tell.

Exercise: Kantian Perspective

Kantian - Are any of the affected parties being treated as a means to an end?

- By not telling the president, Bob is preserving his own reputation and professional image at some potential cost to the president.
- In this way, Bob is using the president as a means to the end of preserving his reputation.
- Therefore, it is Bob's duty to tell.

Exercise: Virtue Theory Perspective



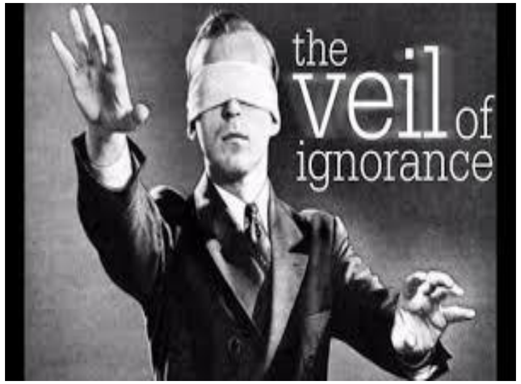
Virtue theory - Does this action violate any moral virtues?

- Honesty is a virtue. Honesty is not limited only to what is said but also to what is left unsaid. Telling partial truths or providing intentionally misleading information, even if technically accurate, is not considered being honest.
- By not telling the president what happened, Bob is not being honest because he is shrewdly withholding information.
- He may even have to avoid bringing up certain aspects of his testing and findings so as to not accidentally be cornered with a pointed question.
- Therefore, Bob should tell.

Exercise: The Veil of Ignorance

The Veil of Ignorance – If Bob had to decide assuming that he was in the president’s shoes, how would this affect his decision?

- By only considering how his actions positively and negatively impact himself, Bob is ignoring half of the equation. If Bob were in the president’s shoes, would he want to know what happened?
- While some might consider ignorance bliss in this situation, many people would want to know if another person possesses private information about them.
- Therefore, Bob should tell.



Example: Facebook Data Mining

- Is it morally acceptable for Facebook to sell highly specific leads to third parties for targeted advertising?

Conditions:

- The affected parties are Facebook and the typical Facebook user
- The action is Facebook mining data for sale to third parties, where that data is based on users' web browsing even beyond Facebook's website
- Sophisticated data mining techniques are used to enable highly specific targeting beyond what the typical user would even expect is possible

Social Responsibility

- The idea that professionals and organizations have an obligation to promote the welfare of society
- Motivation for social responsibility rests on ethical frameworks
- Company slogans like “Don’t be evil” or “Do the right thing” point to a commitment to social responsibility and help remind company employees that ethical concerns are more important than profits
- Do cybersecurity professionals bear any social responsibility for their actions?

Code of Ethics

- Imbues a profession with dignity and elevates the status of those who work in that profession in the eyes of the society
- Provides moral guidance to professionals – it helps to clear up grey areas and fill in gaps where the law is silent
- Removes plausible deniability for those who practice unethical behaviors – they cannot reasonably say that they didn’t know certain actions were considered wrong by their peers

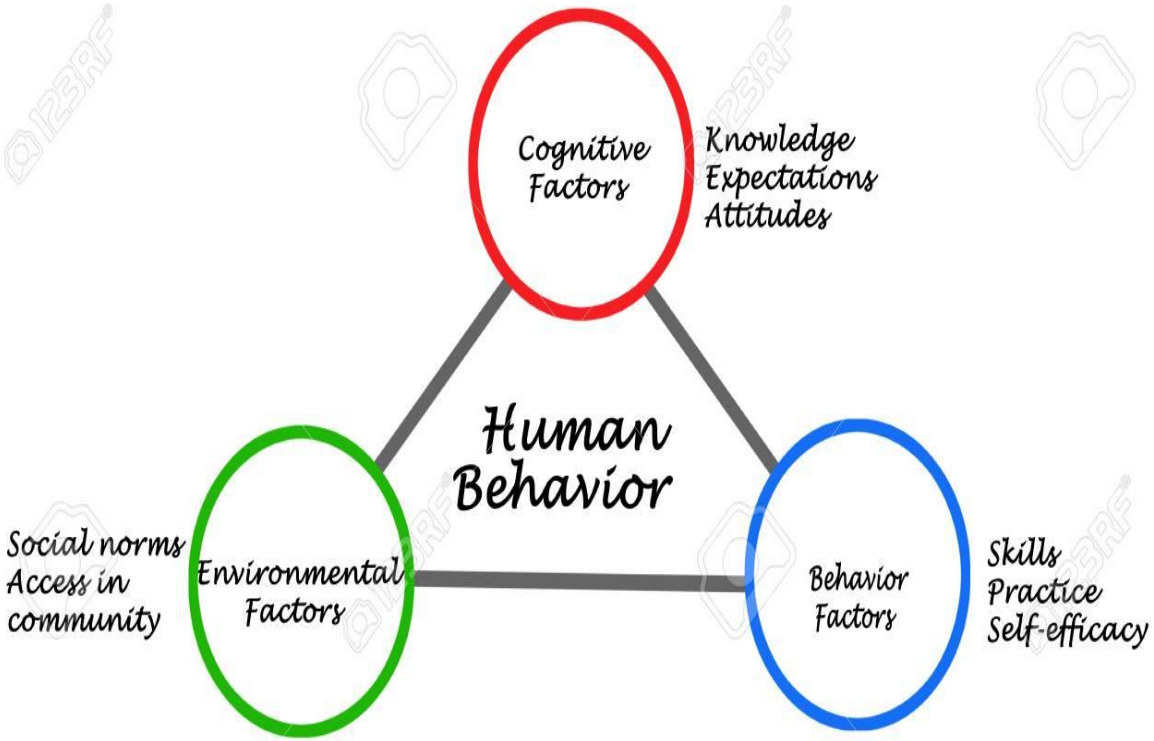
Software Engineering Code of Ethics and Professional Practice

These 9 fundamental principles emerge from the Code:

- Be impartial
- Disclose information that others ought to know
- Respect the rights of others
- Treat others justly
- Take responsibility for your actions and inactions
- Take responsibility for the actions of those you supervise
- Maintain your integrity
- Continually improve your abilities
- Share your knowledge, expertise, and values

Motivating Behavior

- Laws & Rules: prohibit or compel behavior to achieve a societal and an organizational benefit
- Policy: guides actions to those that are most likely to achieve a desired outcome
- Culture: usually unwritten standards for behavior within a group



Standards and Guidelines

Standards are rules

- Used to make policies more effective
- In ICT, will include specifications for software, hardware, or behavior [audit process, i.e.]

Guidelines

- General statements or recommendations
- Best practices / Not mandatory
- NIST SP 800-53 – Security and Privacy Controls http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Creating Policies

Process:

- Identify the problem/desired behavior
- Collect information
- Draft the policy
- Collect feedback
- Implement the policy
- Evaluate the effects of the policy
  - Rinse and repeat…

Elements:

1. Purpose
2. Applicability
3. Effective date (and revision history)
4. Responsibilities
5. Policy statements

If needed

- Background
- Definitions

Elements

1. Purpose

- Explains why the policy is being implemented
- Indicate desired behaviors
- States the problem or conflict the policy is attempting to resolve
- Can the problem or conflict be a common threat?
- Describes the overall benefit of having the policy

2. Applicability

- States who the policy applies to
- Lists who must understand the policy, to be able to perform the job
- Indicates the technologies, groups, and processes included in the policy
- Provides any exceptions to the policy and explains how they are handled
- Can there be overlapping domains of applicability?

Elements (cont'd)

3. Effective rate (revision history)

- Technology changes
- Project rollouts
- New regulatory compliance (or old…)
- Client request; problem discovered
- Expiration (at most two years for a policy)

4. Responsibilities

- Indicates specifically
- Who is needed to make the policy work
- What they need to do
- There may also be an enforcement section of the policy, which indicates penalties for violation of the policy, and who is responsible for administering penalties.

Elements (cont’d)

5. Policy Statements

- Lists behaviors that are being governed
- Lists behaviors required for compliance for individuals covered by the policy
- Provides the general technical requirements for devices and systems to be in compliance
- Policy may include references and pointers to standards and guidelines

Benefits of Policy

- Provide a paper trail of due diligence.
- Exemplify a commitment to security.
- Form a benchmark for progress.
- Help ensure consistency
- Serve as a guide to information security.
- Provide the security team the backing of management.

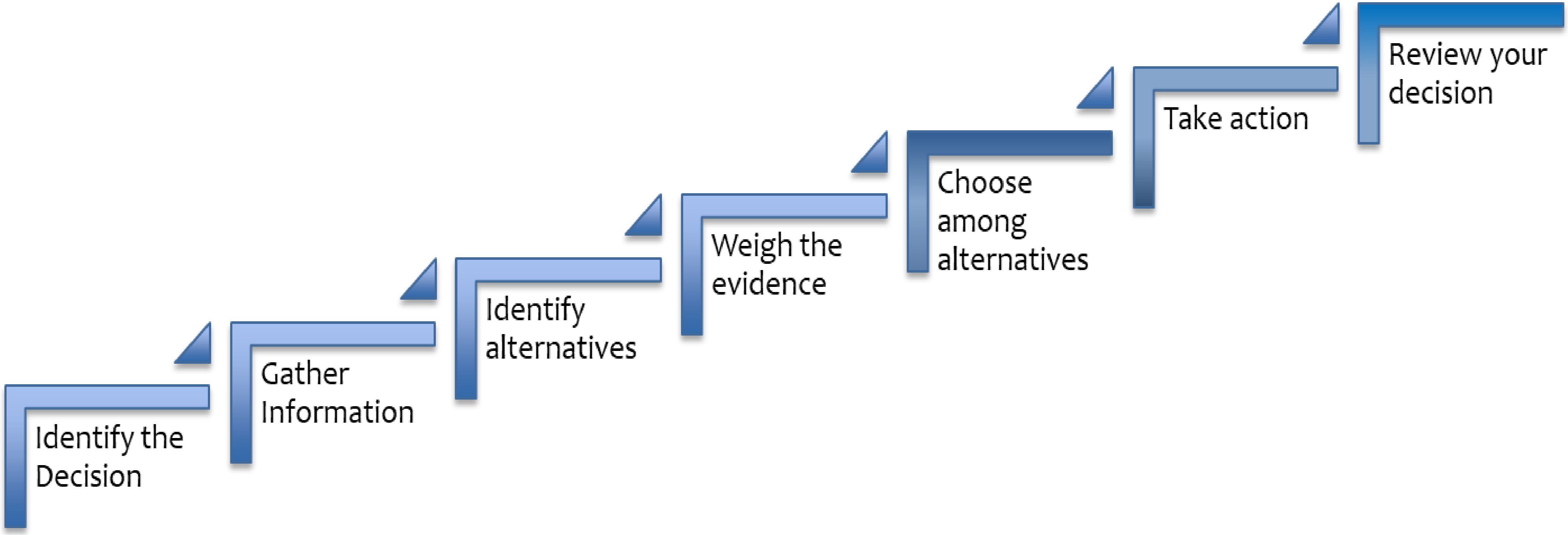
Write a realistic policy

The policy document has to be:

- 1 page only
- Maximum 250 words
- As little as possible technical language
- Shall contain all elements: Purpose, Applicability, Effective date (and revision history), Responsibilities, Policy statements
- With the user in mind (be creative)

Decision Making in Security

- Step-by-step decision-making process



Identify the Decision

Gather Information

Identify alternatives

Weigh the evidence

Choose among alternatives

Take action

Review your decision

MCDM General Criteria for Decision-Making

- As the name implies, Multi-Criteria Decision-Making (MCDM) is about methods – including software – for making decisions when multiple criteria (or objectives) need to be considered together, in order to rank or choose between the alternatives being evaluated.
- In short, MCDM involves these four key components:

1. Alternatives (or individuals) to be ranked or chosen between.
2. Criteria by which the alternatives are evaluated and compared.
3. Weights representing the relative importance of the criteria.
4. Decision-makers (and other stakeholders), whose preferences are to be represented.

Multi Criteria Decision Making Methods

1. Multi-Attribute Utility Theory (MAUT) - expected utility theory that can decide the best course of action in a given problem by assigning a utility to every possible attribute and calculating the best possible utility

Example: a choice between two email phishing filters described on four attributes:

1. security
2. cost
3. latency
4. productivity

Can there be error in elicitation? Simple Multi-Attribute Rating Technique

Multi Criteria (cont’d)

2. Analytic Hierarchy Process (AHP): theory of measurement through pairwise comparisons and relies on the judgments of experts to derive priority scales

Example: a choice between two email phishing filters described on pairwise comparison of four attributes:

1. security
2. cost
3. latency
4. productivity

Multi Criteria (cont'd)

3. Case-Based Reasoning (CBR): CBR is a MCDM method that retrieves cases, similar to a problem, from an existing database of cases, and proposes a solution to a decision-making problem based on the most similar cases.

Example: a choice between two email phishing filters described on four attributes

- A similar case?

Multi Criteria (cont’d)

4. Fuzzy Set Theory: Fuzzy set theory is an extension of classical set theory that “allows solving a lot of problems related to dealing with imprecise and uncertain data”.

Example: a choice between two email phishing filters described on four attributes

- What is the uncertain data?
- Is this MCDM method promising in cybersecurity?

Multi Criteria (cont'd)

5. ELECTRE / PROMETHEE

- ELECTRE: The acronym ELECTRE stands for: ELimination Et Choix Traduisant la REalité (ELimination Et Choice Translating REality). There are two main parts to an ELECTRE application: **First**, the construction of one or several outranking relations, which aims at comparing in a comprehensive way each pair of actions; **Second**, an exploitation procedure that elaborates on the recommendations obtained in the first phase. The nature of the recommendation depends on the problem being addressed: choosing, ranking or sorting.
- PROMETHEE: The Preference Ranking Organization METHod for Enrichment of Evaluations and its descriptive complement geometrical analysis for interactive aid is Based on mathematics and sociology. The method was developed at the beginning of the 1980s. Rather than pointing out a "right" decision, the Promethee method helps decision makers find the alternative that best suits their goal and their understanding of the problem. It provides a comprehensive and rational framework for structuring a decision problem, identifying and quantifying its conflicts and synergies, clusters of actions, and highlight the main alternatives and the structured reasoning behind.

Example: a choice between two email phishing filters described on four attributes

- Importance coefficients? and the veto thresholds?.

Cybersecurity Decision Making Methods

Risk-informed decisions

- All risk factors, stakeholders, and decision criteria
- identified, deconstructed, and understood

Risk-based decisions

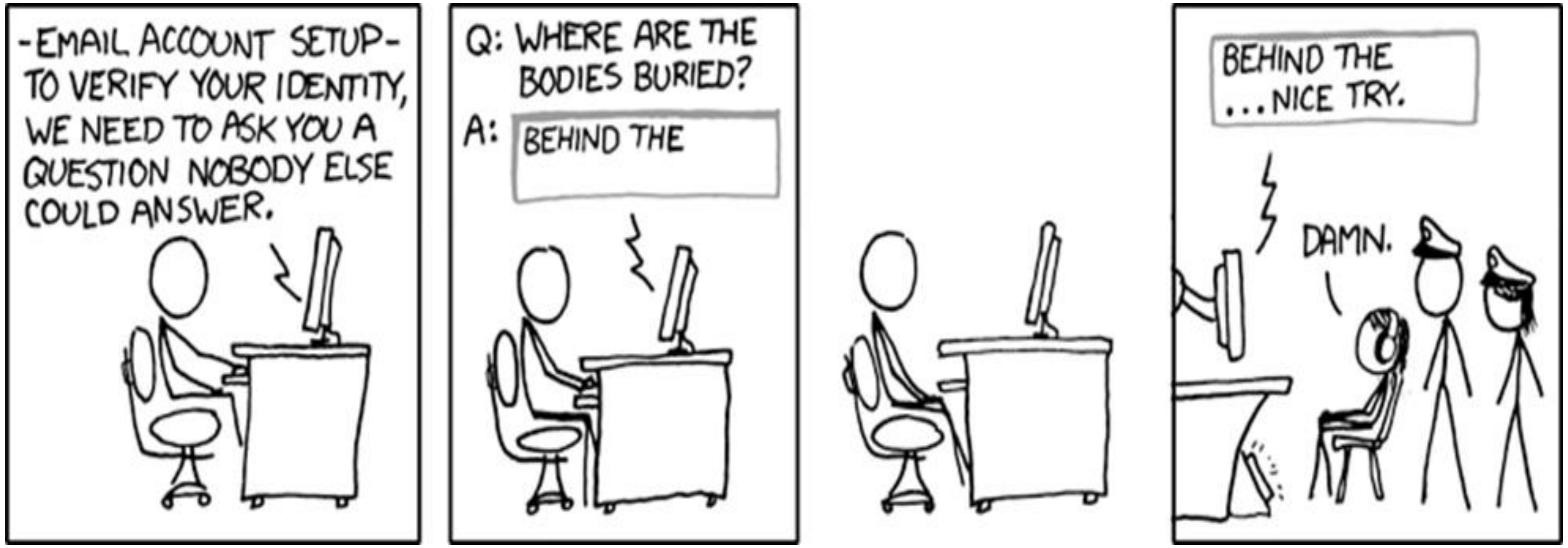
- What we attempt to do :)

Resilience-based decisions

- Capability of the system to absorb, adapt and recover.
- Robustness and sensitivity

A note on SETA

- Security Education, Training and Awareness
- Raise employees' awareness of how best to help protect the organization
- Uses a variety of instructional tools
- SETA is a control, put in place as a result of risk assessment


-EMAIL ACCOUNT SETUP-
TO VERIFY YOUR IDENTITY, WE NEED TO ASK YOU A QUESTION NOBODY ELSE COULD ANSWER.
Q: WHERE ARE THE BODIES BURIED?
A: BEHIND THE
BEHIND THE ...NICE TRY.
DAMN.

A. Awareness

- Used to motivate secure behavior
- Reminds people that security supports the organization’s mission
- Needs to change regularly and creatively, to avoid becoming part of the background
- Used to remind people about
  - Basic security practices
  - Security hygiene

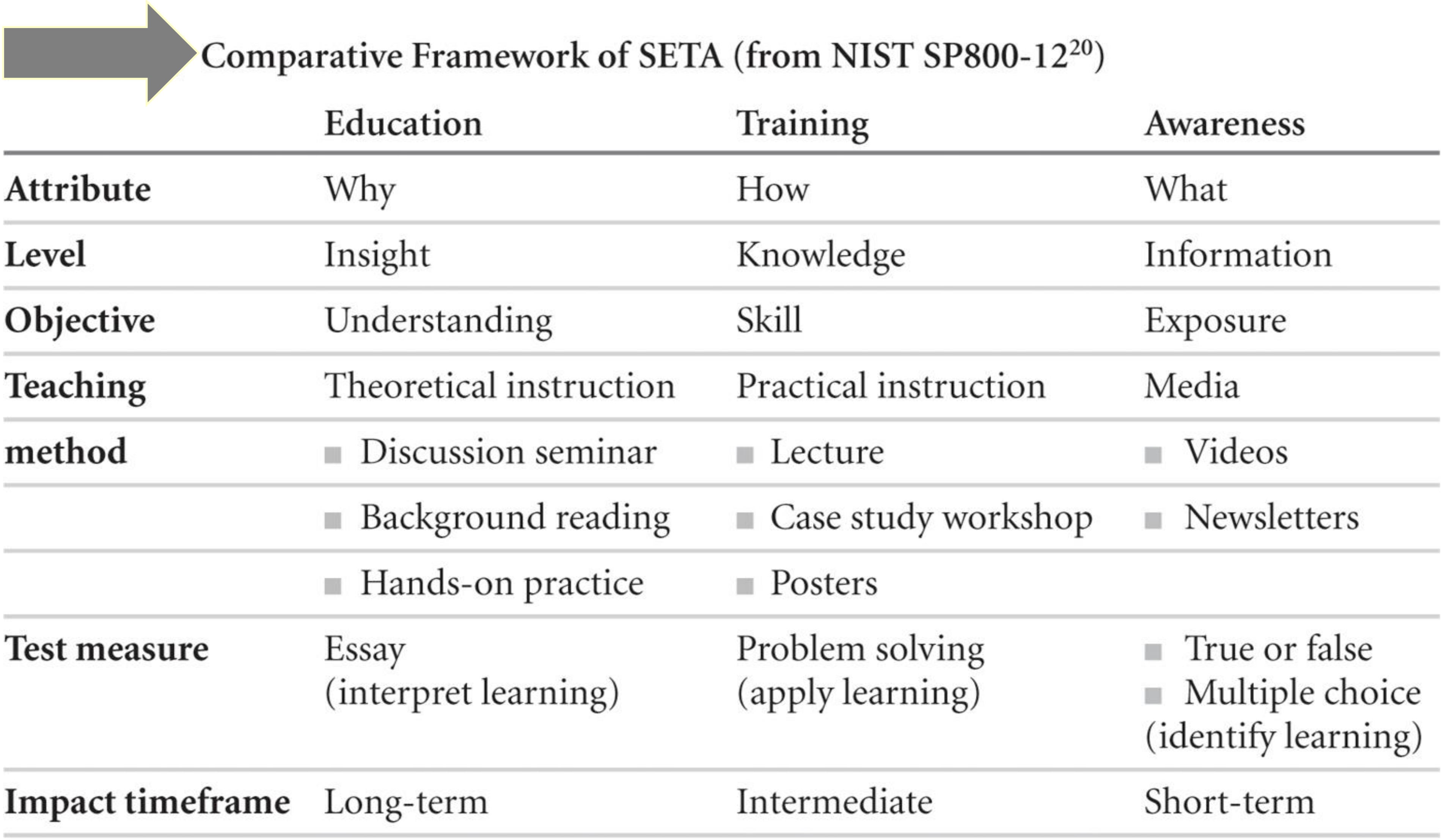
B. Training

- Teaches skills that allow employees to perform their jobs more securely
- Most effective when targeted to specific audiences
- Position
- Technology used
- Can be generally targeted, most effectively for basic security practices

C. Education

- Targeted at security professionals or those whose job requires security expertise
- Career development – continuous improvement
- Graduate programs
- Certificate programs
- Other specialized training programs

SETA Framework



Comparative Framework of SETA (from NIST SP800-12[20])

	Education	Training	Awareness
Attribute	Why	How	What
Level	Insight	Knowledge	Information
Objective	Understanding	Skill	Exposure
Teaching	Theoretical instruction	Practical instruction	Media
method	■ Discussion seminar	■ Lecture	■ Videos
	■ Background reading	■ Case study workshop	■ Newsletters
	■ Hands-on practice	■ Posters	
Test measure	Essay (interpret learning)	Problem solving (apply learning)	■ True or false ■ Multiple choice (identify learning)
Impact timeframe	Long-term	Intermediate	Short-term

Examples

- OpenDNS: https://www.opendns.com/phishing-quiz/
- Sonic Wall https://www.sonicwall.com/en-us/phishing-iq-test

Creating a SETA plan

- Education will likely be beyond the scope of your organization
- Design the program – risk assessment
- Develop the awareness and training material
- Implement the plan
- NIST 800-50
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf
- NIST 800-16
  http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf

SETA Program Design

- Scope of the awareness and training plan
- Roles and responsibilities for the plan
- Goal to be accomplished for each aspect
- Target audience for each aspect
- Learning objectives
- Deployment methods
- Evaluation plan

Recommendations

- Target SETA to address highest ranking concerns of the risk assessment
- Make SETA relevant to employees
- Related to their work
- Related to the types of access they have
- Evaluate the SETA program to ensure it is meeting the needs of the organization
- https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforce-framework-resource-center

Metrics

- Security Responsiveness - Number of Reported Incidents
- Sensitive Data Handling – DLP Violations; Audit for Data Leakage
- Online / Browsing Hygiene – Number of visits to unapproved sites (from web content filter or IDS/IPS)
- Email Hygiene – Email Filter Acceptable User Violations / Abuse
- Phishing resilience – Phishing Audit Susceptibility / Report Rate / Attack Rate
- Passwords – Average Time to Crack / Password Resets
- Insider Threats – Detected Attacks / Reported Incidents
- Working Remotely – Number or % of Attacks while on VPN
- Device Protection - Number of lost devices / PIN resets / avg time to report loss
- Computer Behavior Awareness - % of infections user-reported
- Physical Security – Physical Security Audit

Certification

- Professional development
- Aimed primarily at the security professional
- Ensures that professionals have the required level of knowledge to perform their roles
- Knowledge may be gained through education, job experience, or some combination
- Your recommendation?

2) Videos: Discussion & Reflection

- Brainstorming Techniques
- Ethical Dilemma

Go to the virtual room, and complete the activity thread.

3) Sixth Lab: Comprehensive Project & Practice

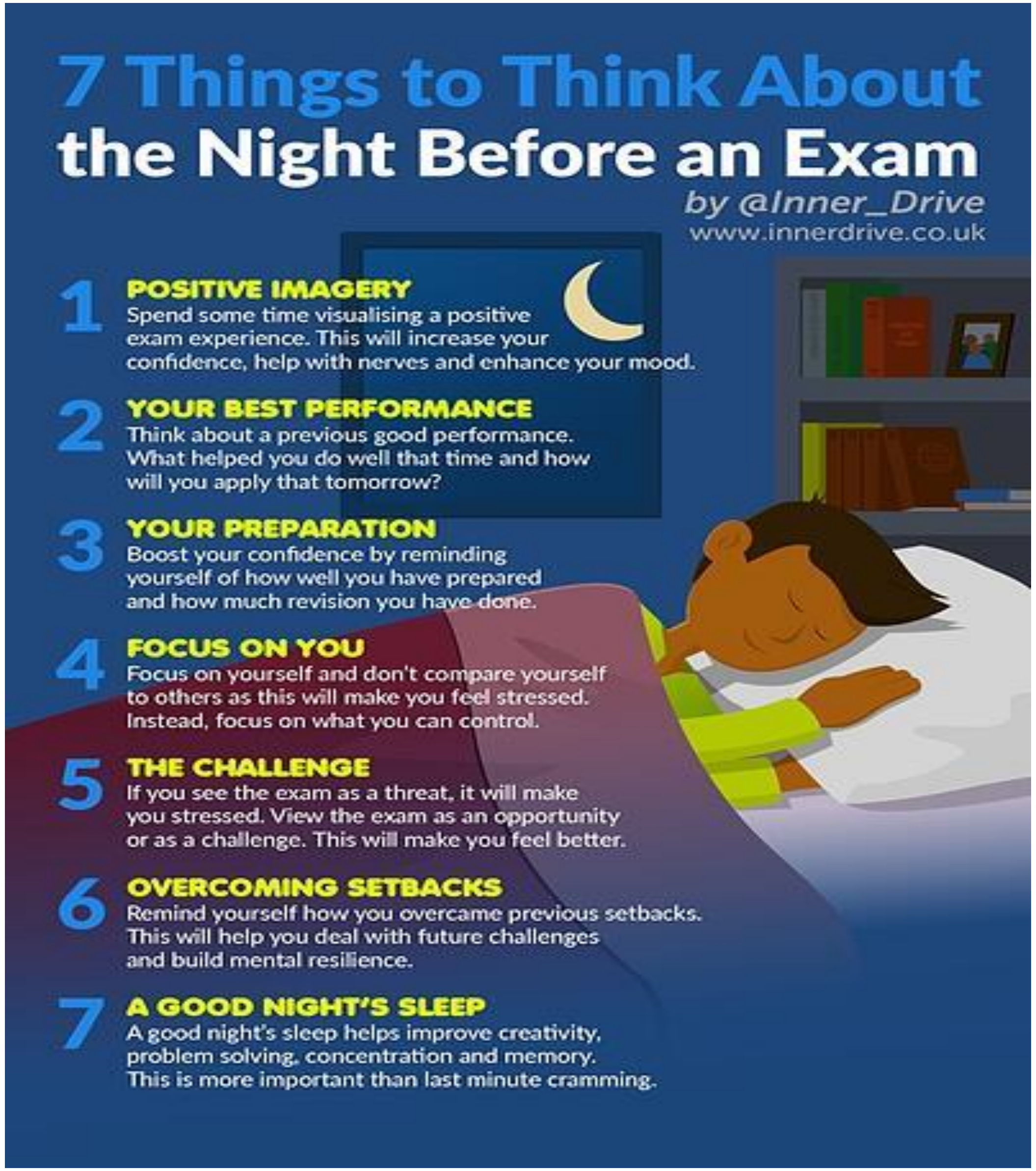
Please go to the Virtual Room for Instructions\\

4) In Closing: Debriefings for Cases

- Debriefing for Cases 01 – 02 – 03 – 04 – 05
- Please go to the *Virtual Room* for Instructions
- Prepare your answers accordingly!

5) Exam

- Time for the Examination
- Instructions will be provided shortly!
- Prepare your answers accordingly!



7 Things to Think About the Night Before an Exam

by @Inner_Drive
www.innerdrive.co.uk

1 **POSITIVE IMAGERY**
Spend some time visualising a positive exam experience. This will increase your confidence, help with nerves and enhance your mood.

2 **YOUR BEST PERFORMANCE**
Think about a previous good performance. What helped you do well that time and how will you apply that tomorrow?

3 **YOUR PREPARATION**
Boost your confidence by reminding yourself of how well you have prepared and how much revision you have done.

4 **FOCUS ON YOU**
Focus on yourself and don't compare yourself to others as this will make you feel stressed. Instead, focus on what you can control.

5 **THE CHALLENGE**
If you see the exam as a threat, it will make you stressed. View the exam as an opportunity or as a challenge. This will make you feel better.

6 **OVERCOMING SETBACKS**
Remind yourself how you overcame previous setbacks. This will help you deal with future challenges and build mental resilience.

7 **A GOOD NIGHT'S SLEEP**
A good night's sleep helps improve creativity, problem solving, concentration and memory. This is more important than last minute cramming.

Until next time!

- *"There is a powerful driving force inside every human being that, once unleashed, can make any vision, dream, or desire a reality."*

  -- Anthony Robbins

Thank you

Day 06

CLOSED

FOR BUSINESS