Information Security and Systems

Jeff Klaben

February 8, 2025

Agenda

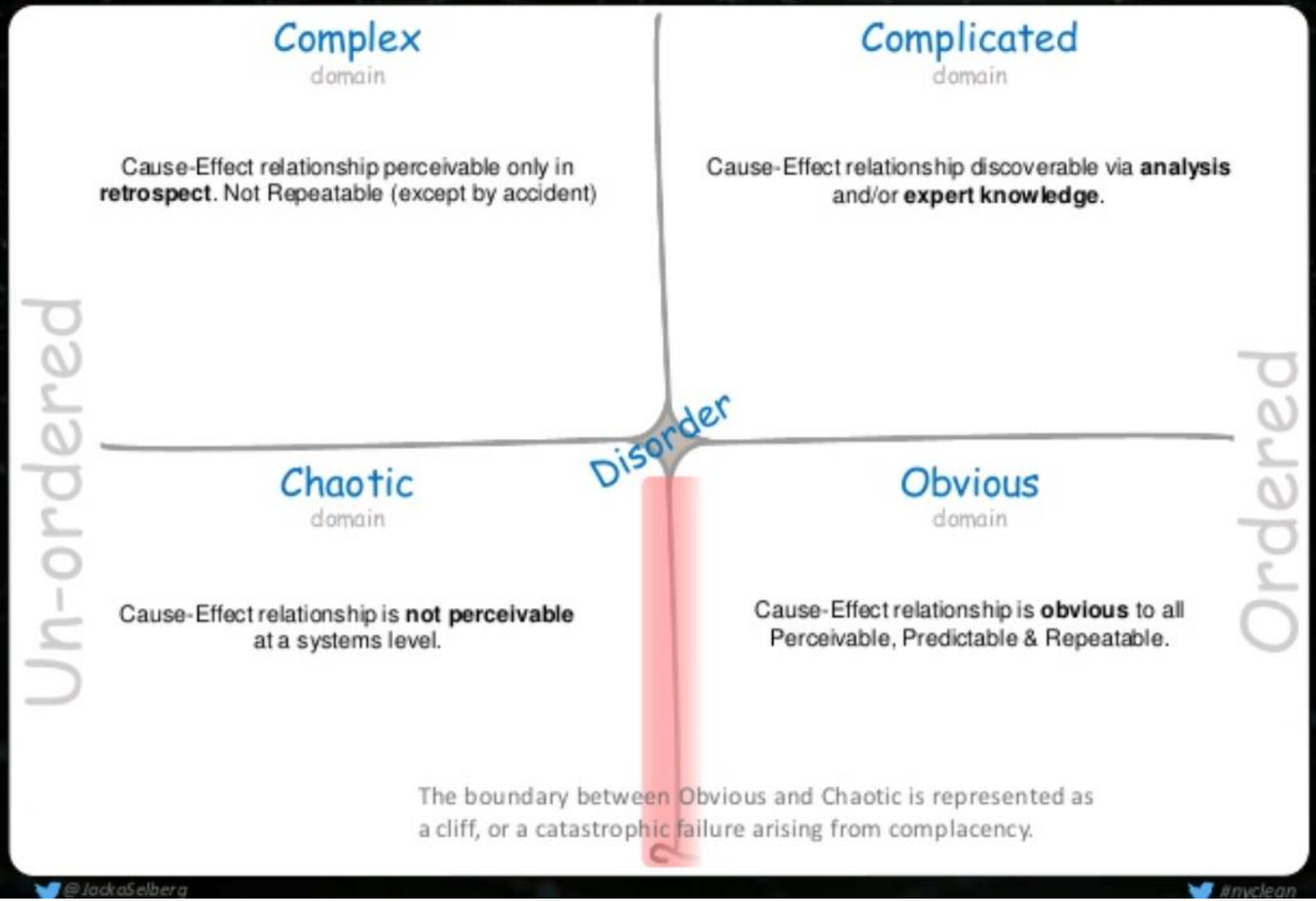
- Discussion: User Stories, Vision
- Lecture: Information Security and Systems
- Break
- Lecture: AI Governance
- Review Fact Pattern 2
- Team working sessions

Building Privacy atop Secure Systems

- Feeling overwhelmed by disorder?
- Need/want structure/focus
  - Specialize to divide and conquer
  - keep talking to each other (EBLC)
- Strategies to deal with perceived overload and imposter syndrome
  - Focus on task at hand (EBLC Simulation Questions)
  - Find common language, values, and organizing principles

Cynefin and Complexity: A Gentle Introduction - *Jocko Selberg*

Introducing the Cynefin Domains



Current EBLC Simulation Questions

- Which opportunities are most promising and which resources / business assets are most valuable to enable us to move forward?

- The legality of the project, and how we can legitimately monetize the data. Specifically, what are the use cases of how we can monetize the data in alignment with our company's goals and visions?

- What are the data privacy implications that need to be considered?

- What are some of the ethical, trust and safety, and reputational/brand impacts to consider? And how do we mitigate them?

- How do we structure our product/service and present the data in order to monetize it, including the information asset, formatting, and categorizing (classifying) of the data?

Vision Statement

Captures the Imagination

East to share

Get's people excited!

Instructions:
Create a vision statement using the format below. Replace text in brackets with your product information

FOR [target customer]

WHO [statement of need]

THE [product name]

IS A [product category]

THAT [product key benefit, compelling reason to buy],

UNLIKE [primary competitive alternative],

OUR PRODUCT [final statement of primary differentiation].

The Product Vision Board

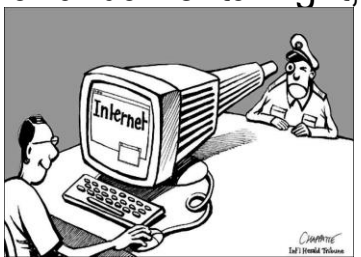
Vision	What is the purpose for creating the product? Which positive change should it bring about?
Target Group	Which market or market segment does the product address? Who are the target customers and users?
Needs	What problem does the product solve? Which benefit does it provide?
Product	What product is it? What makes it stand out? Is it feasible to develop the product?
Business Goals	How is the product going to benefit the company? What are the business goals?

Did / could your team create this structure to articulate your vision?

Common language to discuss Privacy

- In 1928, Supreme Court Justice Louis Brandeis defined privacy as "the right to be left alone":
  - The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. … They knew that only a part of the pain, pleasure and satisfaction of life are to be found in material things. … They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be left alone—the most comprehensive of rights and the right most valued by civilized men. [1]
- One of the "conditions favorable to the pursuit of happiness."
- One of the conditions necessary for the development of individual identity, for the establishment of intimacy, and for the functioning of democracy.
- Focusing on informational privacy, computer scientist Michael McFarland, SJ, wrote:
  - Reverence for the human person … as an autonomous being requires respect for personal privacy. To lose control of one's personal information is in some measure to lose control of one's life and one's dignity. Therefore, even if privacy is not in itself a fundamental right, it is necessary to protect other fundamental rights.

https://www.scu.edu/ethics/privacy/defining-privacy/



Current EBLC Simulation Questions

- How and where we should store the data, including encryption of the data and who in the company should have access to the data?
- What security controls should we consider and employ, such as a disaster recovery plan, unauthorized access prevention, and data leak management?
- How should we deliver the product/service to potential clients (hosted or non-hosted)?
- How do we manage access to the data in a way to control and limit access on an as-needed basis, and have a tiered permission management model?

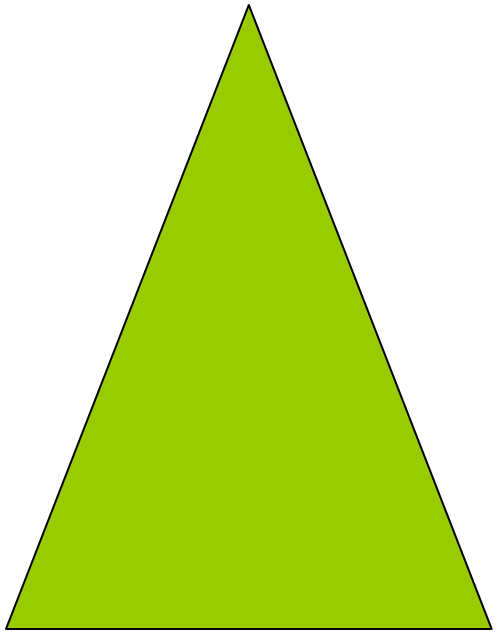
Discussion

- Additional information is required?
- What data sets do you wish you could add?
- Options to pivot?

Questions for next funding meeting:

1. What data products will you offer?
2. How will the data will be provided?
3. What services/reports will be available?
4. Where will the data, and reports/services be hosted?
5. What is the authenticity of the data, how often is your data refreshed?
6. What is your process to keep the data updated and relevant?
7. How do we integrate with your services?
8. What consents or notifications do we need from our users to utilize your services?

Security



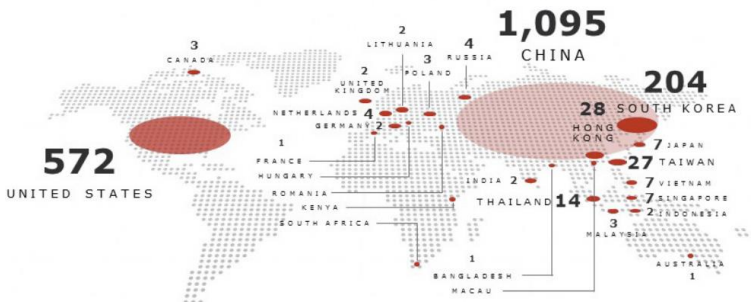
“Attack him where he is unprepared, appear where you are unexpected”
— Sun Tzu

Evolving Threat Characteristics

Multi-vector

Low and Slow

Targeted



Monetized

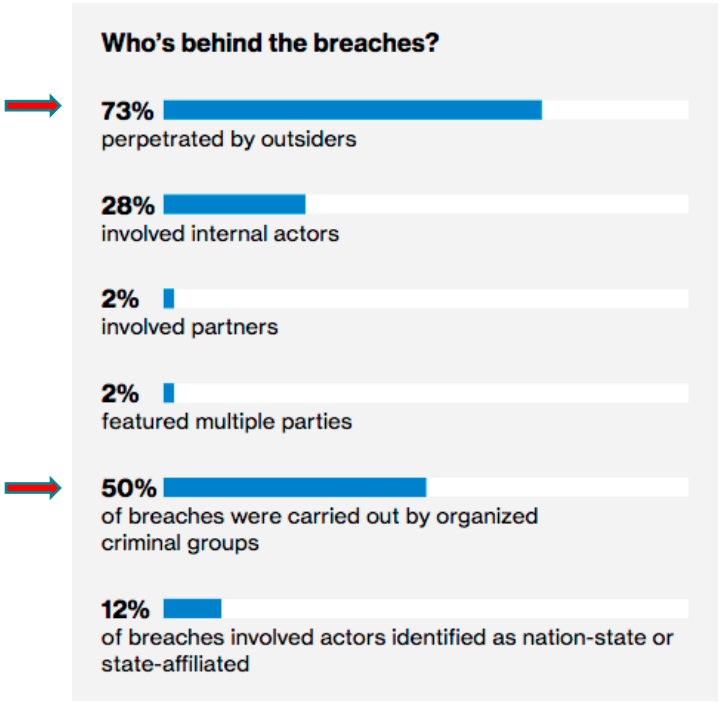
Evasive

Nation State

Low Tech/Phishing

Sources: https://krebsonsecurity.com/tag/deep-panda/; Gartner - Evolving attack techniques and corresponding risk management strategies

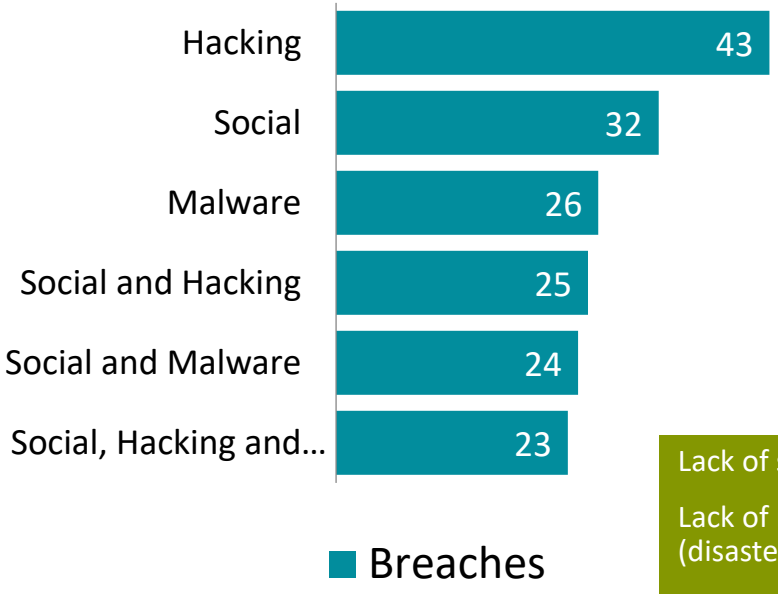
"It is said that if you know your enemies and know yourself, you will not be imperiled in a hundred battles; if you do not know your enemies but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperiled in every single battle. "
— Sun Tzu



Source: Verizon 2018 Data Breach Investigations Report 10th Edition

*"Know the Enemy and Know **Yourself**"*
— Sun Tzu

Education Industry Survey*



Lack of security awareness

Lack of response plan (disaster and recovery plan)

Healthcare Industry Survey*

Privilege Misuse, Miscellaneous Errors and Physical Theft and Loss represent 80% of breaches within Healthcare

Lack of stricter access controls (e.g. Segregation of Duties)

Lack of backup and recovery (to avoid ransomware)

Lack of logging monitoring to detect misuse of privilege

Lack of data classification

* Source: The Cyber Resilient Organization: Learning to Thrive against Threats; Ponemon Institute LLC

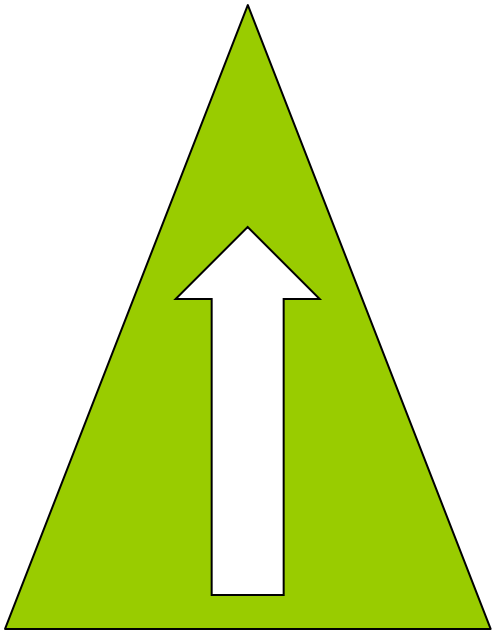
*"Know the Enemy and Know **Yourself**"*
— Sun Tzu

Common Weaknesses:

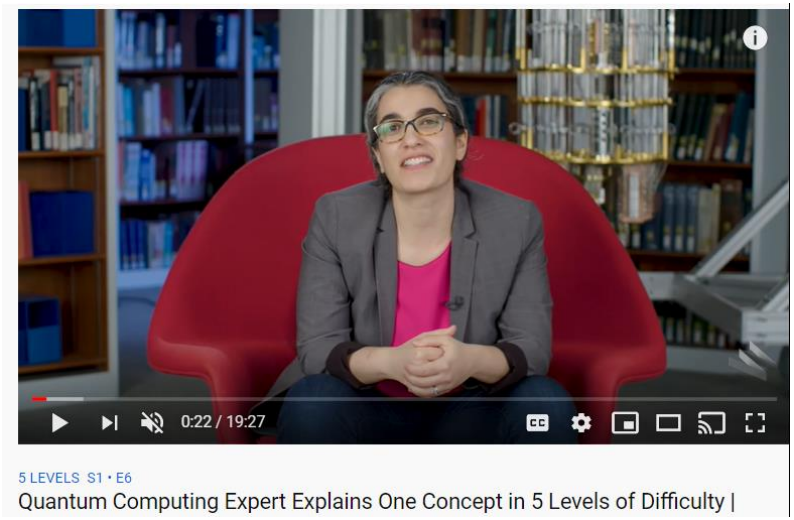
- Human errors
- Lack of planning and preparedness
- Lack of collaboration among business functions
- Organizational factors hinder efforts to achieve a high level of cyber resilience
- Lack of agility
- Lack of technologies that enable efficient backup and disaster recovery operations

Source: The Cyber Resilient Organization: Learning to Thrive against Threats; Ponemon Institute LLC

Levels of Abstraction



- https://youtu.be/OWJCfOvochA



- https://youtu.be/hYip_Vuv8J0

What is Security?

- "The quality or state of being secure—to be free from danger"
- An effective organization *should* have multiple kinds of security in place:
  - Physical security
  - Personal security
  - Operations security
  - Communications security
  - Computer Network security
  - Information security

What is Security? (continued)

- Security goals or services as defined by CNSS (Committee on National Security Systems), is the C.I.A. triangle:
  - **confidentiality, integrity**, and **availability**
- Necessary enforcement tools: policy, awareness, training, education, technology
- C.I.A. triangle now expanded into list of critical characteristics of information

Definitions

- Control objective: A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.
- Control or safeguard: something employed to defend against a threat
- Exploit: a technique used to compromise a system.
- Exposure: exposure exists when there is a vulnerability that is known to a potential attacker
- Risk: potential for loss
- Threat agent: an object, person, or other entity that represents an ongoing danger to an asset
- Vulnerability: a weakness in a particular system that might be exploited by a threat in an attack to cause harm to the system

Critical Characteristics of Information

- The value of information comes from the characteristics it possesses:
  - Availability – available to authorized users
  - Accuracy – free from mistake or error
  - Authenticity – genuine or original rather than fabricated
  - Confidentiality – only allow access by authorized individuals

Integrity

  - Integrity – whole and uncorrupted; has not been modified by a person of lower security rating
  - Utility - if information is available, but not in a format meaningful to the end user, it is not useful
  - Possession - The quality or state of having ownership or control of some object or item.

CNSS (NSTISSC) Security Model

McCumber Cube

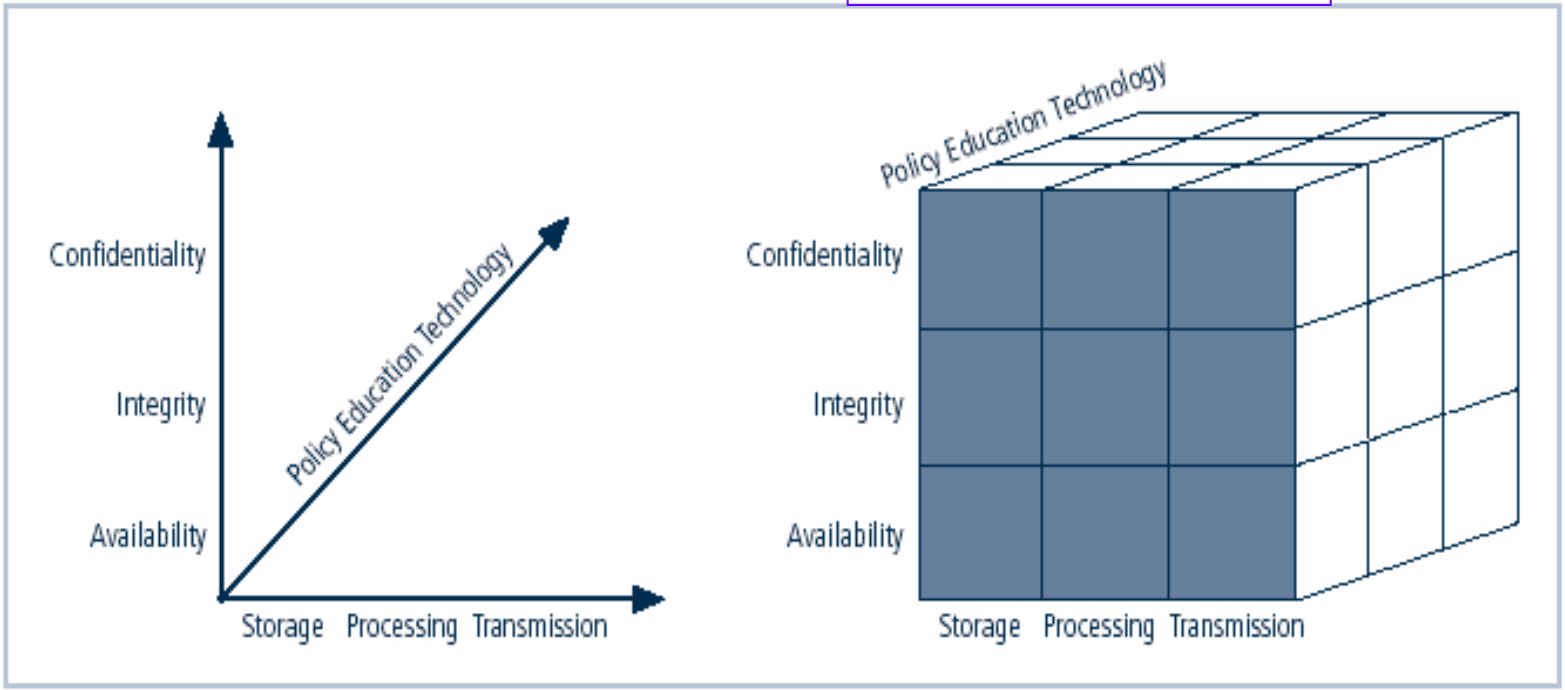


FIGURE 1-4 NSTISSC Security Model

information states, security goals, and means of control

Components of an Information System *(consider in your EBLC solution design)*

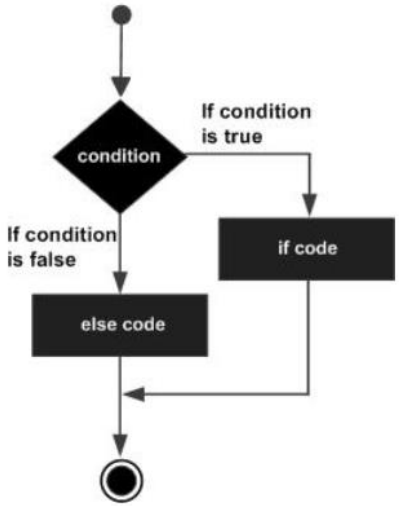
- Information system (IS) is entire set of
  - software
  - hardware
  - data
  - people
  - procedures
  - and networks
- All of these are needed to use information as a resource in the organization and should be considered **assets**

Components of an Information System

- Software (Code)
  - Applications, operating systems, utilities
  - Bugs and vulnerability to viruses, worms, other attacks
- Hardware
  - Computers, PDA's, monitors, cables, keyboards, laptops, CD's
  - Threats: Theft, damage
- Data
  - About employees, about customers, about products
  - Threats: Theft, damage, errors, DBMS provides some security

Code is Not Scary

Flow Diagram




```
if(boolean_expression) {
   /* statement(s) will execute if the boolean expression is true */
} else {
   /* statement(s) will execute if the boolean expression is false */
}
```

Live Demo

```
#include <stdio.h>

int main () {

   /* local variable definition */
   int a = 100;

   /* check the boolean condition */
   if( a < 20 ) {
      /* if condition is true then print the following */
      printf("a is less than 20\n" );
   } else {
      /* if condition is false then print the following */
      printf("a is not less than 20\n" );
   }

   printf("value of a is : %d\n", a);

   return 0;
}
```

```
a is not less than 20;
value of a is : 100
```

Components of an Information System

- People
  - Employees who know the business are an asset; good customers, vendors, etc.
  - Threats are accidents, bribes, inside jobs, cognitive limitations
- Procedures
  - Business procedures are usually company confidential; ex. What to do about lost passwords; telephone lists
- Networks
  - System accessibility and availability
  - Business decision: include network hardware and software?

Balancing Information Security and Access

- Impossible to obtain “perfect or 100% security” — it is a process, not an absolute
- Security should be considered a balance between protection and availability
- To achieve balance, level of security must allow reasonable access, yet protect against threats
  - Example: must change password every 30 days

“Victory usually goes to the army who has better trained officers and wo/men.”
— Sun Tzu

Basic IAM Stack

- Centralized Identity repository
- Strong authentication
- Lifecycle management
- Privileged Access Management

…enables these IAM capabilities

- Stricter password controls
- Stricter defense for
- Automated controls
- Strong Authentication

- Single Sign On
- Unified policy for on-prem, cloud and mobile
- Role based access controls
- Centralized reporting

- Self service password management
- Protection against brute force and denial or service
- Improved visibility
- Integration with existing security tools

The Systems Development Life Cycle

- Systems Development Life Cycle (SDLC) is methodology for design and implementation of information system within an organization
- Methodology is formal approach to problem solving based on structured sequence of procedures
- Using a methodology:
  - Ensures a rigorous process
  - Avoids missing steps
- Goal is creating a comprehensive security posture/program
- Traditional SDLC consists of six general phases

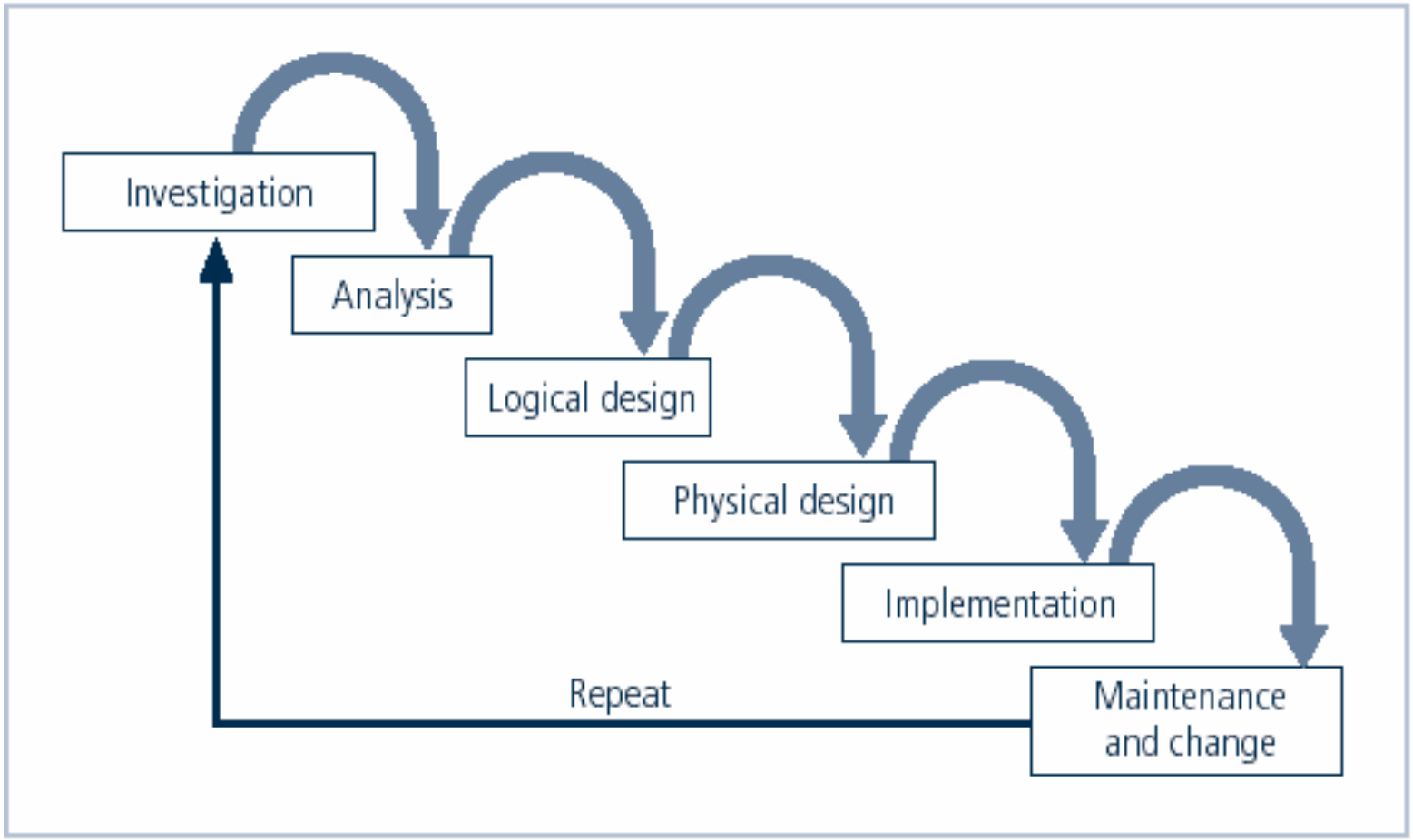


FIGURE 1-9 SDLC Waterfall Methodology

Investigation

- What problem is the system being developed to solve?
- Objectives, constraints, and scope of project are specified
- Estimate costs, evaluate existing resources and develop preliminary cost-benefit analysis
- At the end, feasibility analysis is performed to assess economic, technical, and behavioural feasibilities of the process

Analysis

- Consists of assessments of the organization, status of current systems, and capability to support proposed systems
- Develop preliminary system requirements
- Analysts determine what new system is expected to do and how it will interact with existing systems
- Ends with documentation of findings and update of feasibility analysis

Logical Design

- Main factor is **business need**; applications capable of providing needed services are identified and evaluated
- Data support and structures capable of providing the needed inputs are identified
- Technologies to implement physical solution are determined
- Multiple solutions are considered
- Feasibility analysis performed/updated at the end

Physical Design

- The "best" solution is selected (based on criteria)
- Technologies to support the alternatives identified and evaluated in the logical design are selected
- Components evaluated on make-or-buy decision
- Feasibility analysis updated; entire solution presented to end-user representatives for approval

Implementation

- Needed software is created; components ordered, received, assembled, and tested
- Users trained and documentation created
- Feasibility analysis updated
- Users presented with system for performance review and acceptance test

Maintenance and Change

- Consists of tasks necessary to support and modify system for remainder of its useful life
- Life cycle continues until the process begins again from the investigation phase
- When current system can no longer support the organization's mission, a new project is implemented
- Longest and most expensive phase

Adding Security Considerations

- Traditional SDLC **should be** enhanced to include security (your task is to make sure of this)
- Some tasks belong to more than one phase or could be done in more than one phase
- Investigation/Analysis phases
  - Preliminary Risk Assessment – define threat environment and security needs
  - Security Categorization – define level of impact of a breach of security in proposed system

Adding Security Considerations

- Logical/Physical Design Phases
  - Risk Assessment – more in-depth and specific
  - Security Requirements Analysis
  - Cost of information security reporting
  - Security Plan – contingency plan, incident response plan, security awareness and training plan, authorizations and accreditations
  - Select and develop security controls; develop security test and evaluation plan

Adding Security Considerations

- Implementation Phase
  - Inspection and Acceptance – ensure that security functionality is included in deliverables
  - Systems Integration – ensure system integration process includes security (and privacy) considerations
  - Security Certification and Accreditation – follow security certification procedures to provide assurance

Adding Security Considerations

- Maintenance and Change Phase
  - Configuration Management and Control
  - Continuous monitoring of controls
  - Information Preservation – ensure that information is retained as needed to meet legal requirements and accommodate future technology changes that may make the retrieval method obsolete
  - Media Sanitization – ensure that data is appropriately destroyed
  - Hardware and software disposal plan/policy

The Security Systems Development Life Cycle

- The same phases used in traditional SDLC may be adapted to support specialized security implementation or IS plan and program
- Identification of specific threats and creating controls to counter them
- SecSDLC is a coherent program that can be used to guide many processes

Investigation and Analysis

- Investigation
  - Identifies goals and constraints of the project
  - Develop Enterprise Information Security Policy (EISP)
- Analysis
  - Analysis of existing security policies or programs, along with documented current threats and associated controls
  - Includes analysis of relevant legal issues (privacy laws, HIPAA, Gramm-Leach-Bliley, etc.) that could impact design of the security solution
  - Risk management task begins with Risk Identification

Logical Design and Physical Design

- Logical Design
  - Develop “information security blueprint”
  - Select Risk Control strategies and develop risk mitigation plans:
    - Business Continuity planning
    - Incident response
    - Disaster recovery
  - Feasibility analysis: should project be continued or outsourced
- Physical Design
  - Needed security technology is evaluated, and final design is selected
  - Develop criteria for determining effectiveness of the solution

Implementation and Maintenance, Change

- Implementation
  - Security solutions are acquired, tested, implemented, and tested again
  - Personnel issues evaluated; training and education programs conducted
  - Entire tested package is presented to management for final approval
- Maintenance and Change
  - Perhaps the most important phase given the ever-changing threat environment
  - Constantly monitor, test, update and repair to meet changing threats

“Let your plans be dark and impenetrable as night, and when you move, fall like a thunderbolt”
— Sun Tzu

Initiating
- Formal recognition of the beginning of a project
- A description of the product of the project, initial documentation of project objectives and assignment of a project manager

Planning
- Creating and maintaining a workable plan to accomplish the purpose of the project
- A documented project plan and documented updates to the plan as the project progresses

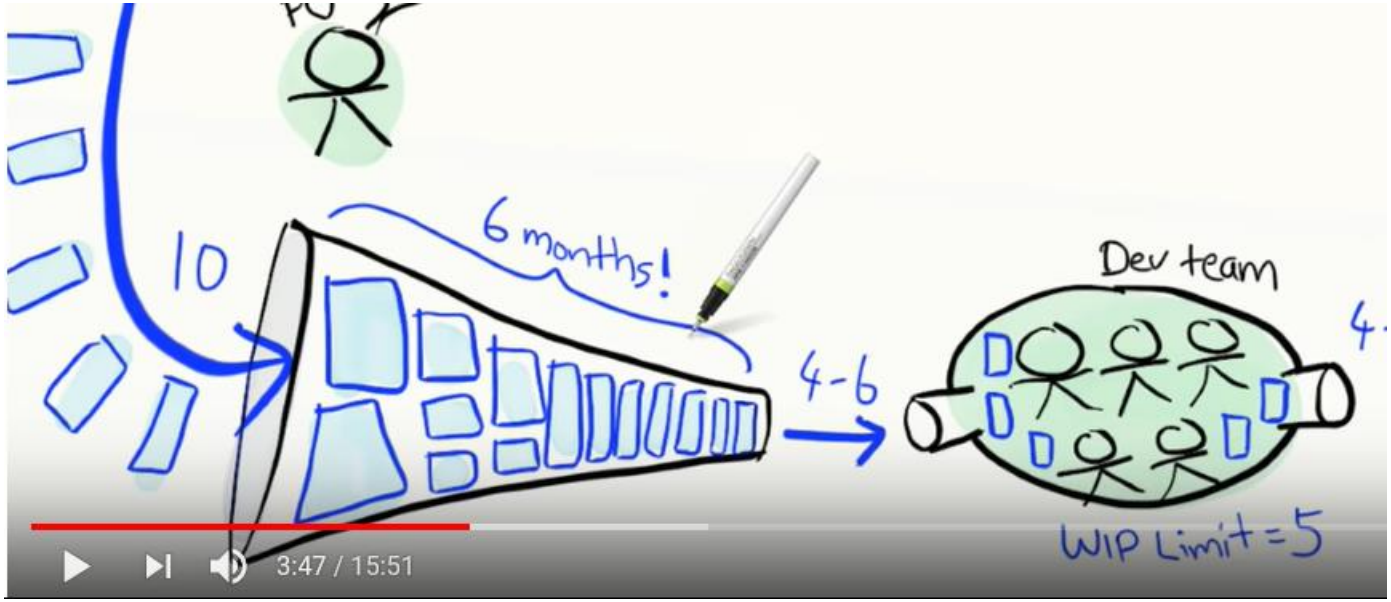
Executing
- Carrying out the plan
- Verifiable completed project deliverables

Controlling
- Monitoring progress and taking corrective action when necessary
- Periodic measurements of progress vs. plan, corrective action when needed and identification of when the project is done

Closing
- Bringing project and paperwork to 100% completion, and entering the history in a database
- Documented acceptance of the results of the project

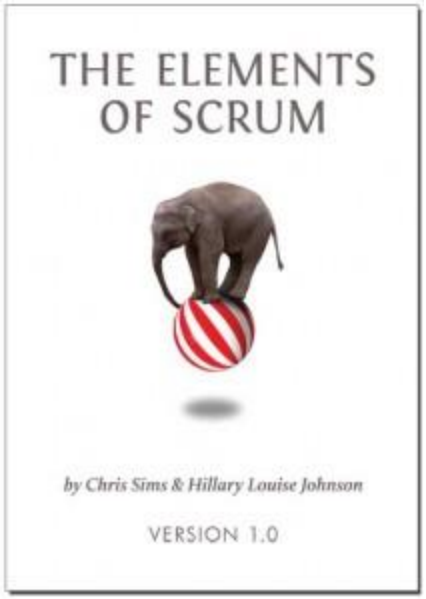
Agile Product Ownership in a Nutshell

- https://youtu.be/502ILHjX9EE



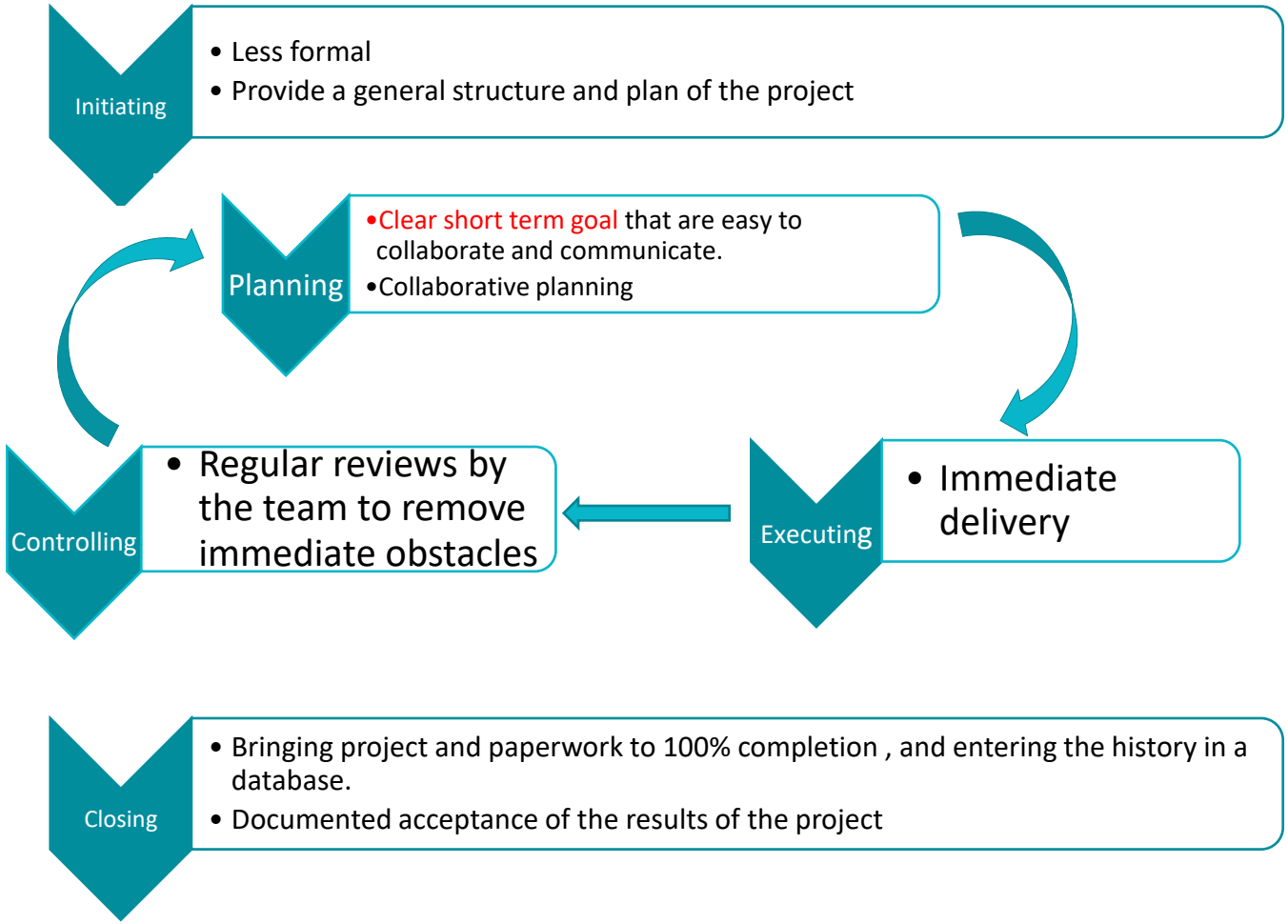
Agile

- http://www.agilelearninglabs.com/
  - Video: Scrum in 13 Minutes

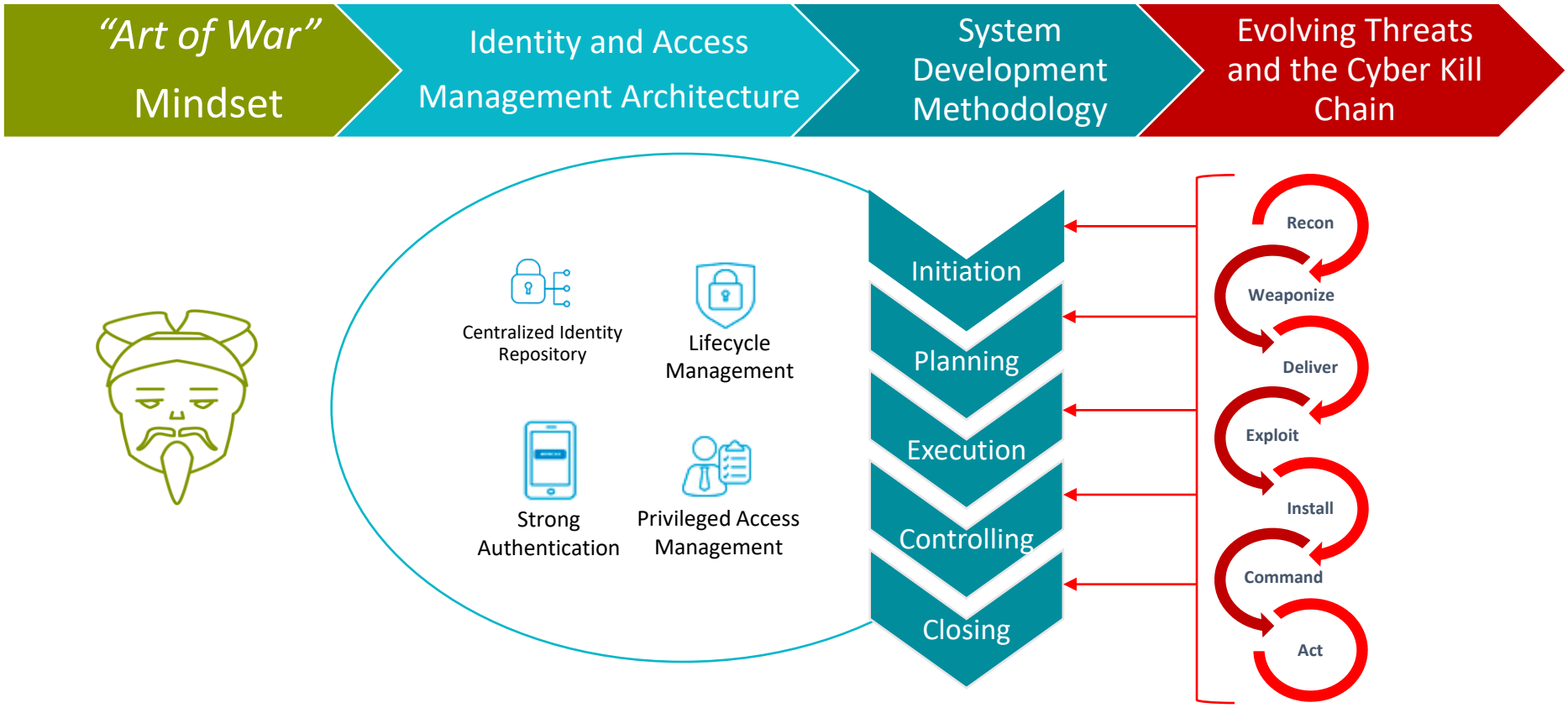


"Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat."

— Sun Tzu



Goal: Enhance resilience during and post deployment of IAM* systems



*IAM: Identity and Access Management

Feb 22 Guest Speaker:

Arda Ozdemir

In the last 15 years, working with over 6,000 clients, I've developed practical, life-changing tools and techniques that help you live a better, healthier and happier life.

Improve your Relationship with my 7 Communication Strategies

Discover your Innate Gifts and Become the Best Version of Yourself