

# İTÜ Computer Security

## Human Factors

Dr. Şerif Bahtiyar

1

## Before Starting

How 'the invisible network' poses a major security threat



If a hacker managed to switch off a life-support machine, the results could be fatal

<http://www.bbc.com/news/business-41252203>

16.10.2024

Human Factors

2

2

## Outline

- Security Awareness, Training, and Education
- Employment Practices and Policies
- E-Mail and Internet Use Policies
- Computer Security Incident Response Teams

16.10.2024

Human Factors

3

3

## Security Awareness, Training, and Education

- Human resource security
- A **significant** topic for computer security and application security
- Full discussion is beyond this course



16.10.2024

Human Factors

4

4

## Security Awareness, Training, and Education

### Some Standards

- ISO27002 (Code for Practice for Information Security Management)
- NIST 800-100 (Information Security Handbook: A Guide for Managers)
- **PCI DSS** v3 (Payment Card Industry Data Security Standard)



16.10.2024

Human Factors

5

5

## Security Awareness, Training, and Education

- **Employee behavior** is a **critical concern** in ensuring the security of computer systems and information assets.
- **Motivation**: the programs provide **4 major benefits**
  1. **Improving employee** behavior
  2. Increasing the ability to hold the employees **accountable** for their actions
  3. **Mitigating liability** of the organization for an employee's behavior
  4. **Complying** with **regulations** and contractual obligations

16.10.2024

Human Factors

6

6

## Security Awareness, Training, and Education

- Problems associated with employee behavior
  - Errors
  - Omissions
  - Fraud
  - Actions by disgruntled employees
- Security awareness, training, and education programs can reduce the problems of
  - Errors and
  - Omissions



16.10.2024

Human Factors

7

7

## Security Awareness, Training, and Education

- Employees cannot be expected to follow policies and procedures of which they are unaware.
- Enforcement is more difficult if employees can claim ignorance when caught in a violation.
- The programs
  - Limit an organization's liability
  - Comply with regulations and contractual obligations, such as access to clients' data



16.10.2024

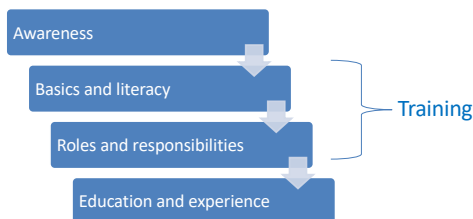
Human Factors

8

8

## Security Awareness, Training, and Education

- There is a need for a continuum of learning programs that starts with awareness, builds to training, and evolves into education.
- NIST SP 800-16



16.10.2024

Human Factors

9

9

## Security Awareness, Training, and Education

A security awareness program seeks to inform and focus an employee's attention on issues related to security within one organization.



16.10.2024

Human Factors

10

10

## Security Awareness, Training, and Education

### Benefits of awareness

- Employees are aware of their responsibilities regarding security and act accordingly
- Employees understand the significance of relation between security and the organization
- Promotes support to security staff recruitments and security products

16.10.2024

Human Factors

11

11

## Security Awareness, Training, and Education

### Awareness

- Attribute: what is allowed or not allowed but not how
- Level: information
- Objective: recognition
- Teaching method: media, such as videos, newsletters, posters, etc. (identify learning)
- Test measure: true/false or multiple choice
- Impact timeframe: short term

16.10.2024

Human Factors

12

12

## Security Awareness, Training, and Education

### Some Goals of security awareness programs

- Rise staff **awareness** in **general**
- Ensure that staff are aware of **governmental laws** and **regulations** related to security
- **Organizational** security policies and procedures
- Ensure that staff understand the **significance** of a **sole employee**
- Train staff according to their **positions**
- Inform staff that they are **monitored**
- Remind the **consequences** of security **breaches**
- Teach the significance of **reporting**
- Create a **trusted** system



16.10.2024

Human Factors

13

13

## Security Awareness, Training, and Education

An organization should have a **security awareness policy**, which

- For every **employee** there should be an **orientation** program and **periodic** activities
- Everyone should have (given) **time** to participate the activities
- **Responsibilities** should be clearly **defined**.



16.10.2024

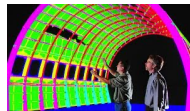
Human Factors

14

14

## Security Awareness, Training, and Education

- A **security training program** teaches people the skills to **perform** their information system related **tasks** **more securely**.



- Depending on the role of the user, training **includes basic** and **advanced** computer skills.

16.10.2024

Human Factors

15

15

## Security Awareness, Training, and Education

For **general user**, **training** focuses on **good computer security practices**

- Protecting the **physical** area and equipments (DVD, locking doors, etc)
- Protecting **authentication** credentials (passwords, PINs, tokens)



- **Reporting** security **violations** and **incidents**

16.10.2024

Human Factors

16

16

## Security Awareness, Training, and Education

**Programmers, developers, and system maintainers** require more **specialized** or **advanced** **training**.



**Problem:** They **do not understand** how to do **security** related **tasks**

16.10.2024

Human Factors

17

17

## Security Awareness, Training, and Education

The **training objectives** for these group

- Develop a security **mindset** in the developer
- Show **how** to **build** security into development life cycle
- Teach the developer **how attackers exploit** software and **how to resist** attack.
- Provide **analysis** with a toolkit of **specific** attacks and principles with which to interrogate systems.



16.10.2024

Human Factors

18

18

## Security Awareness, Training, and Education

- **Management-level** should teach managers
  - **How** to make trade-offs among **risk, cost, and benefits**
  - Need to **understand** the **development lifecycles**
  - Use the security **checkpoints** and **evaluation** techniques
- **Executive level** should teach
  - **Difference** between **software security** and **network security**
  - Understand security **risks and costs**
  - Understand security **measurement** and **awareness**

16.10.2024

Human Factors

19

19

## Security Awareness, Training, and Education

### Training

- **Attribute:** **how** to ...
- **Level:** **knowledge**
- **Objective:** **skill**
- **Teaching method:** **practical** instruction (lecture, case study workshop,...)
- **Test measure:** problem solving (**apply learning**)
- **Impact timeframe:** **intermediate**

16.10.2024

Human Factors

20

20

## Security Awareness, Training, and Education

- The **most in-depth** program in security **education**.
- This is **targeted** at security **professionals** and those jobs require **expertise** in security.
- **Education**
  - **Attribute:** **why**
  - **Level:** **insight**
  - **Objective:** **understanding**
  - **Teaching method:** **theoretical** instructions (discussion seminars, background reading)
  - **Test measure:** essay (**interpret learning**)
  - **Impact timeframe:** **long-term**



16.10.2024

Human Factors

21

21

## Security Awareness, Training, and Education

	Awareness	Training	Education
Attribute	"What"	"How"	"Why"
Level	Information	Knowledge	Insight
Objective	Recognition	Skill	Understanding
Teaching method	Media <ul style="list-style-type: none"> <li>– Videos</li> <li>– Newsletters</li> <li>– Posters, etc.</li> </ul>	<b>Practical instruction</b> <ul style="list-style-type: none"> <li>– Lecture</li> <li>– Case study workshop</li> <li>– Hands-on practice</li> </ul>	<b>Theoretical instruction</b> <ul style="list-style-type: none"> <li>– Discussion seminar</li> <li>– Background reading</li> </ul>
Test measure	True/false Multiple choice (identify learning)	Problem solving (apply learning)	Essay (interpret learning)
Impact timeframe	Short term	Intermediate	Long term

16.10.2024

Human Factors

22

22

## Employment Practices and Policies

- A **large majority** of significant **computer crime** are **individuals** who have **legitimate access** now, or who have recently had access.
- **Managing personnel** with potential access is an **essential part** of information security.



16.10.2024

Human Factors

23

23

## Employment Practices and Policies

**Employees** can be involved in **security violations** in a one of two ways:

- **Failing** to follow procedures
- **Knowingly** violates procedures



16.10.2024

Human Factors

24

24

## Employment Practices and Policies

Some **threats** from internal users:

- Gaining unauthorized access
- Altering data
- Deleting production and backup data
- Crashing or destroying systems
- Misusing systems
- Stealing strategic data



16.10.2024

Human Factors

25

25

## Employment Practices and Policies

**Background checks** and **screening** (for **Hiring Process**)

- **Hiring** presents **management** with significant **challenges**.



- A **significant number of employers** have a **corporate policy** that **forbids discussing** a former employee's performance in any way, **positive** or **negative**.
- Despite obstacles, **employers** must make a **significant effort**

16.10.2024

Human Factors

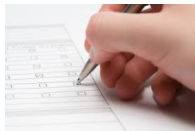
26

26

## Employment Practices and Policies

General **guidelines** for **checking applicants**:

- Ask for more **details** and **educational history**
- Investigate the **accuracy** of details
- Arrange **experienced staff** members to interview candidates



16.10.2024

Human Factors

27

27

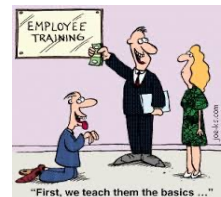
## Employment Practices and Policies

- **During employment**, there are **two** elements of personnel security:

- Security **policy document**
- An ongoing **awareness** and **training program** for all employees.

- **Principles** for personnel security (ISO 27002):

- **Least privilege**
- **Separation of duties**
- Limited reliance on **key employees**



16.10.2024

Human Factors

28

28

## Employment Practices and Policies

- **Termination of employment**: The termination **process** is **complex** and depends on
  - the **nature** of the organization
  - the **status** of employee
  - the **reason** for departure



- Some **important actions**:
  - **Removing** the person from **authorized access lists**
  - **Removing** person's **access codes**
  - **Notifying** departments and related people, such as guards

16.10.2024

Human Factors

29

29

## E-Mail and Internet Use Policies

A growing number of companies **incorporate specific e-mail and Internet use policies** into the organization's security policy.



16.10.2024

Human Factors

30

30

## E-Mail and Internet Use Policies

### Motivation

- Significant employee **time** may be consumed in a **non-work-related** activities (surfing, game)
- Excessive** and **casual** use of **Internet** and **e-mail** increases the **risk** of introducing **malicious** software
- Non-work-related** activity could result in **liability** problems with other organizations
- They may be used by an employee to **harm** another employee
- May damage **reputation** of the organization

16.10.2024

Human Factors

31

31

## E-Mail and Internet Use Policies

Some **policy issues** regarding **e-mail and Internet use** :

- Business use only
- Reasonable personal use
- Policy scope
- Content ownership
- Privacy
- Unlawful activity prohibited
- Security policy
- Company policy
- Company rights
- Disciplinary actions



16.10.2024

Human Factors

32

32

## Computer Security Incident Response Teams

- The **development of procedures to respond to computer incidences** is regarded as an **essential** control for most organizations.
- The incident handling and response procedures **need to**
  - reflect** the range of possible **consequences** of an incident on the organization
  - allow** for a suitable **response**.



16.10.2024

Human Factors

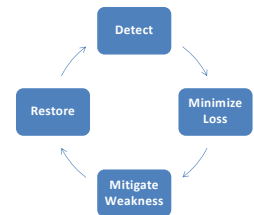
33

33

## Computer Security Incident Response Teams

For a **large** and **medium-sized** organizations, a computer incident response team (CSIRT) is **responsible** for

- Rapidly **detect** incidents
- Minimizing** loss and destruction
- Mitigating** the weakness
- Restoring** computer services



16.10.2024

Human Factors

34

34

## Computer Security Incident Response Teams

**Benefits** of **incident response capability** (NIST SP 800-61)

- Systematically **response**
- Recover** quickly and **minimize** loss
- Handle **future** incidents
- Dealing properly with **legal** issues



16.10.2024

Human Factors

35

35

## Computer Security Incident Response Teams

- A **good incident response policy** should
  - Indicate** the **action**
  - Specify** the **personnel**
  - Detail** the **contacts** of personnel for quick decision making
- Security incidents** are generally **categorized**:
  - Unauthorized **access** to a system
  - Unauthorized **modification** of information

16.10.2024

Human Factors

36

36

## Computer Security Incident Response Teams

### Security Incident Terminology

- **Artifact**: something used to attack the system (virus, exploit)
- **Computer security incident response team (CSIRT)**
- **Constituency**: The group of users, sites, networks, or organizations served by the CSIRT
- **Incident**: A violation of computer security policies or standard security practices
- **Triage**: The process of receiving, initial sorting, and prioritizing of information to facilitate its appropriate handling.
- **Vulnerability**: A characteristic of a piece of information which can be exploited to perpetrate a security incident.

16.10.2024

Human Factors

37

37

## Computer Security Incident Response Teams

- **Detecting incidents**: Incidents can be detected by staff or automated tools.
- **Incident detecting tools** include
  - System integrity verification tools
  - Log analysis tools
  - Network and host intrusion detection tools (IDS)
  - Intrusion prevention systems
- The effectiveness of automated tools depends on the accuracy of their configuration, and the correctness of the patterns and signatures used.



16.10.2024

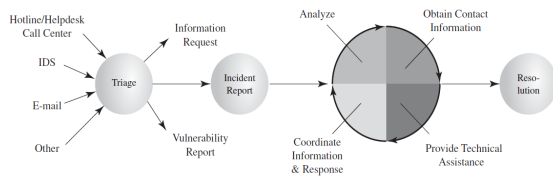
Human Factors

38

38

## Computer Security Incident Response Teams

**Triage function** ensures that all information destined for the incident handling service is channeled through a single focal point regardless of the method by which it arrives for appropriate redistribution and handling within the service.



16.10.2024

Human Factors

39

39

## Computer Security Incident Response Teams

- **Responding to incidents**: Response procedures must deal how to identify the cause of the security incident, whether accidental or deliberate.
- In determining the appropriate responses to an incident, a number of issues should be considered, such as:
  - How critical the system is
  - The current and potential technical effects

16.10.2024

Human Factors

40

40

## Computer Security Incident Response Teams

- Some potential response activities:
  - Take action to protect systems and networks
  - Rebuilding systems
  - Patching or repairing systems
  - Developing response strategies
- **Documenting Incidents**: There is a need to identify what vulnerability led to its occurrence and how this might be addressed to prevent the incident in the future.

16.10.2024

Human Factors

41

41

## Summary

- Employee behavior
- Problems with employee behavior
- Security awareness, training, and education
- Employment practices and policies
- E-mail and Internet use policies
- Computer security incident response

16.10.2024

Human Factors

42

42