Computer Security: Principles and Practice

Fourth Edition, Global Edition

By: William Stallings and Lawrie Brown

Chapter 17

Human Resources Security

Security Awareness, Training, and Education

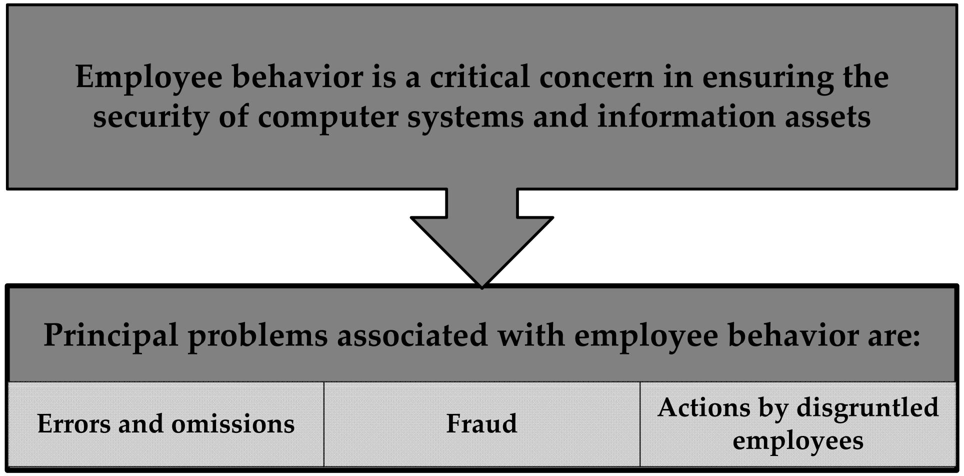
The topic of security awareness, training, and education is mentioned prominently in a number of standards and standards-related documents, including ISO 27002 (*Code of Practice for Information Security Management) and* NIST SP 800-100 (*Information Security Handbook: A Guide for Managers).*

Benefits to Organizations

Security awareness, training, and education programs provide four major benefits to organizations:

- Improving employee behavior
- Increasing employee accountability
- Mitigating liability for employee behavior
- Complying with regulations and contractual obligations

Human Factors



Employee behavior is a critical concern in ensuring the security of computer systems and information assets

Principal problems associated with employee behavior are:

Errors and omissions	Fraud	Actions by disgruntled employees

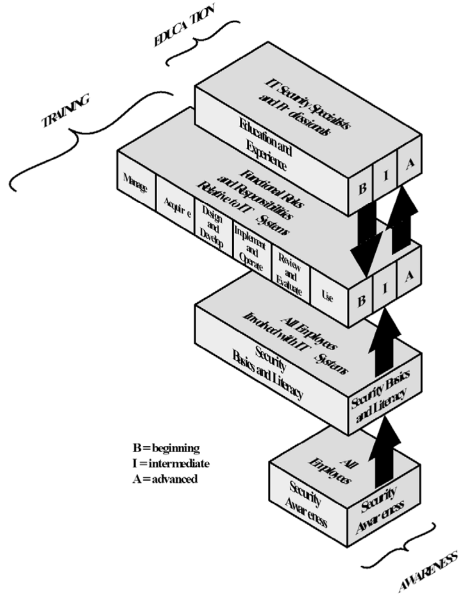


Figure 17.1 Information Technology (IT) Learning Continuum

Table 17.1
Comparative Framework

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

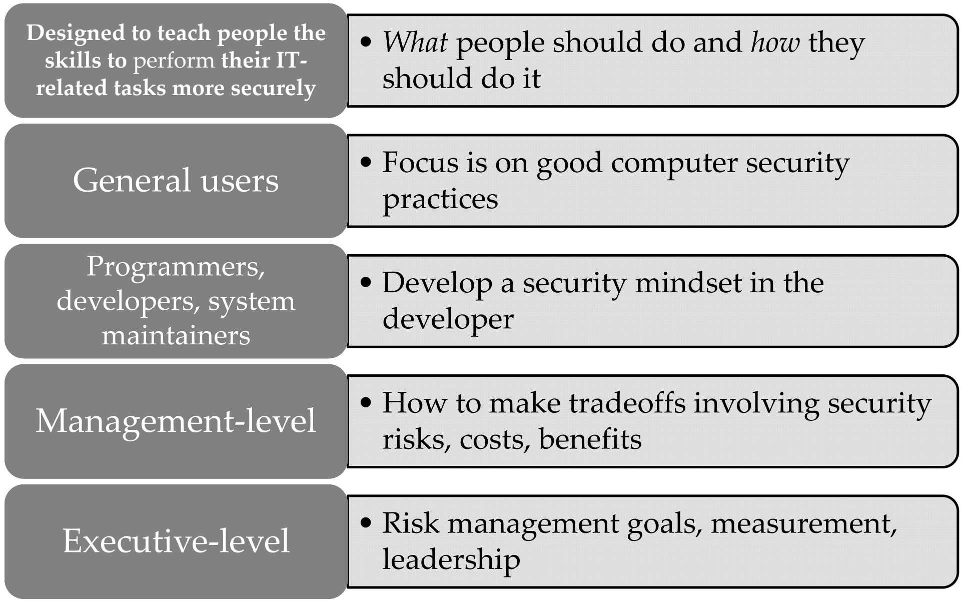
Awareness

- Seeks to inform and focus an employee's attention on security issues within the organization
  - Aware of their responsibilities for maintaining security and the restrictions on their actions
  - Users understand the importance of security for the well-being of the organization
  - Promote enthusiasm and management buy-in
- Program must be tailored to the needs of the organization and target audience
- Must continually promote the security message to employees in a variety of ways
- Should provide a security awareness policy document to all employees

NIST SP 800-100 (*Information Security Handbook: A Guide for Managers*) describes the content of awareness programs, in general terms, as follows:

> "Awareness tools are used to promote information security and inform users of threats and vulnerabilities that impact their division or department and personal work environment by explaining the *what* but not the *how* of security, and communicating what is and what is not allowed. Awareness not only communicates information security policies and procedures that need to be followed, but also provides the foundation for any sanctions and disciplinary actions imposed for noncompliance. Awareness is used to explain the rules of behavior for using an agency's information systems and information and establishes a level of expectation on the acceptable use of the information and information systems."

Training



Designed to teach people the skills to perform **their IT-related tasks more securely**

- *What* people should do and *how* they should do it

General users

- Focus is on good computer security practices

Programmers, developers, system maintainers

- Develop a security mindset in the developer

Management-level

- How to make tradeoffs involving security risks, costs, benefits

Executive-level

- Risk management goals, measurement, leadership

Education

- Most in depth program
- Targeted at security professionals whose jobs require expertise in security
- Fits into employee career development category
- Often provided by outside sources
  - College courses
  - Specialized training programs

Employment Practices and Policies

- Managing personnel with potential access is an essential part of information security
- Employee involvement:
  - Unwittingly aid in the commission of a violation by failing to follow proper procedures
  - Forgetting security considerations
  - Not realizing that they are creating a vulnerability
  - Knowingly violate controls or procedures

Security in the Hiring Process

- Objective:
  - "To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities"
- Need appropriate background checks and screening
  - Investigate accuracy of details
- For highly sensitive positions:
  - Have an investigation agency do a background check
  - Criminal record and credit check

Employment Agreements

Employees should agree to and sign the terms and conditions of their employment contract, which should include:

I. Employee and organizational responsibilities for information security

II. A confidentiality and non-disclosure agreement

III. Reference to the organization's security policy

IV. Acknowledgement that the employee has reviewed and agrees to abide by the policy

During Employment

Objectives with respect to current employees:

- Ensure that employees, contractors, and third-party users are aware of information security threats and concerns and their responsibilities and liabilities with regard to information security
- Are equipped to support the organizational security policy in their work
- Reduce the risk of human error

Two essential elements of personnel security during employment are:

- A comprehensive security policy document
- An ongoing awareness and training program

Security principles:

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

Termination of Employment

- Termination security objectives:
  - Ensure employees, contractors, and third party users exit organization or change employment in an orderly manner
  - The return of all equipment and the removal of all access rights are completed

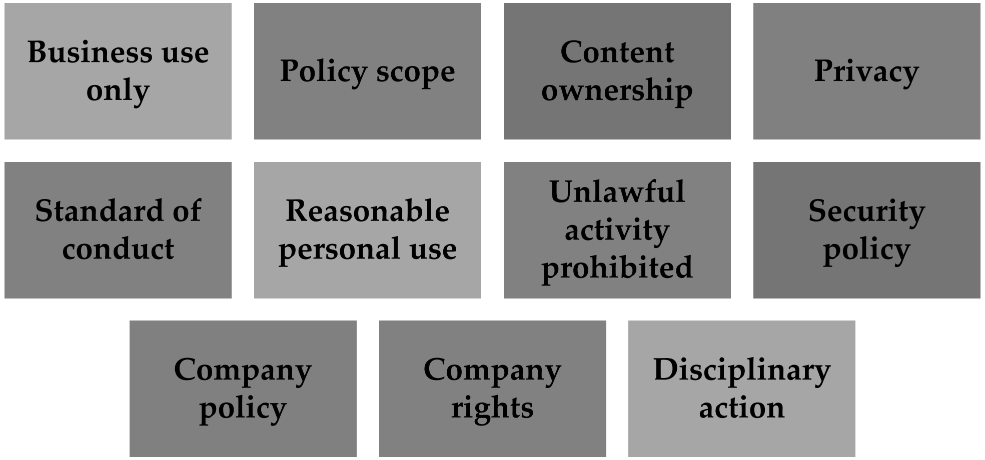
Critical actions:

- Remove name from all authorized access lists
- Inform guards that ex-employee general access is not allowed
- Remove personal access codes, change physical locks and lock combinations, reprogram access card systems
- Recover all assets, including employee ID, portable USB storage devices, documents, and equipment
- Notify by memo or e-mail appropriate departments

Email and Internet Use Policies

- Organizations are incorporating specific e-mail and Internet use policies into their security policy document
- Concerns for employers:
  - Work time consumed in non-work-related activities
  - Computer and communications resources may be consumed, compromising the mission that the IT resources are designed to support
  - Risk of importing malware
  - Possibility of harm, harassment, inappropriate online conduct

Suggested Policies



Business use only

Policy scope

Content ownership

Privacy

Standard of conduct

Reasonable personal use

Unlawful activity prohibited

Security policy

Company policy

Company rights

Disciplinary action

Security Incident Response

- Response procedures to incidents are an essential control for most organizations
  - Procedures need to reflect possible consequences of an incident on the organization and allow for a suitable response
  - Developing procedures in advance can help avoid panic
- Benefits of having incident response capability:
  - Systematic incident response
  - Quicker recovery to minimize loss, theft, disruption of service
  - Use information gained during incident handling to better prepare for future incidents
  - Dealing properly with legal issues that may arise during incidents

Computer Security Incident Response Team (CSIRT)

CSIRTs are responsible for:

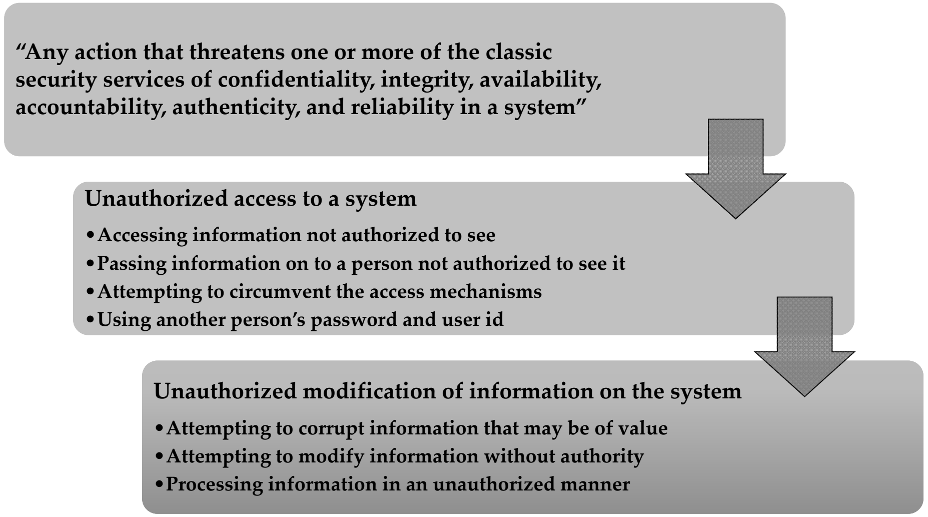
Rapidly detecting incidents

Minimizing loss and destruction

Mitigating the weaknesses that were exploited

Restoring computing services

Security Incidents



"Any action that threatens one or more of the classic security services of confidentiality, integrity, availability, accountability, authenticity, and reliability in a system"

Unauthorized access to a system

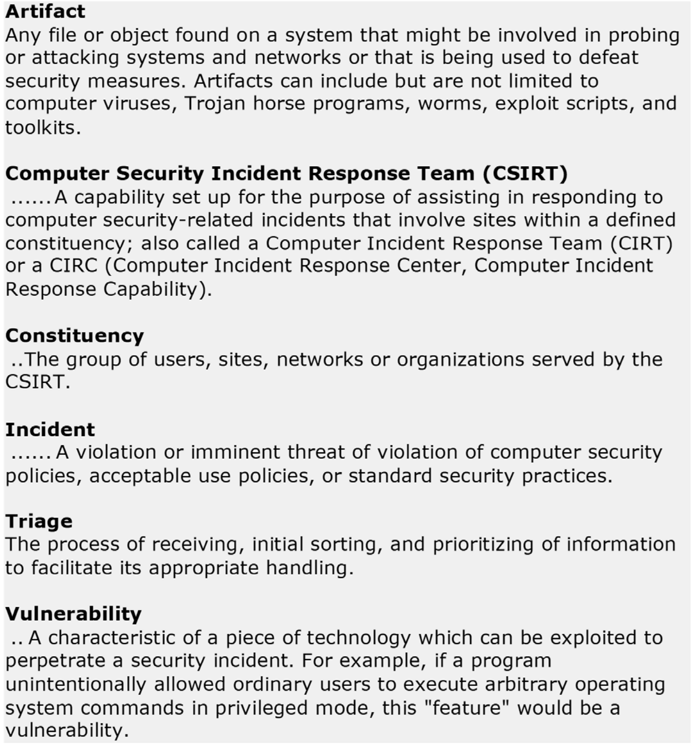
- Accessing information not authorized to see
- Passing information on to a person not authorized to see it
- Attempting to circumvent the access mechanisms
- Using another person's password and user id

Unauthorized modification of information on the system

- Attempting to corrupt information that may be of value
- Attempting to modify information without authority
- Processing information in an unauthorized manner

Table 17.2

Security Incident Terminology



Artifact
Any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures. Artifacts can include but are not limited to computer viruses, Trojan horse programs, worms, exploit scripts, and toolkits.

Computer Security Incident Response Team (CSIRT)
......A capability set up for the purpose of assisting in responding to computer security-related incidents that involve sites within a defined constituency; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability).

Constituency
..The group of users, sites, networks or organizations served by the CSIRT.

Incident
...... A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

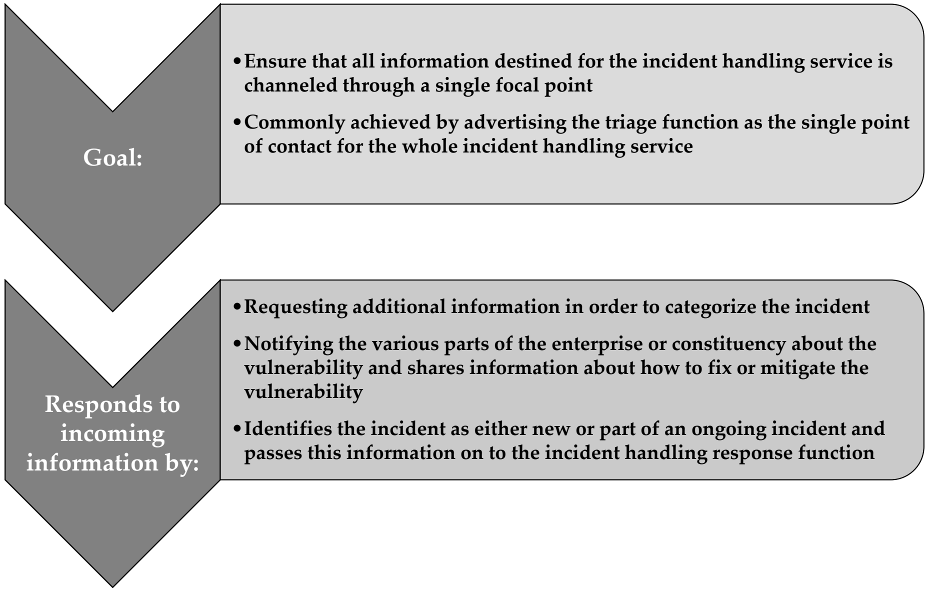
Triage
The process of receiving, initial sorting, and prioritizing of information to facilitate its appropriate handling.

Vulnerability
.. A characteristic of a piece of technology which can be exploited to perpetrate a security incident. For example, if a program unintentionally allowed ordinary users to execute arbitrary operating system commands in privileged mode, this "feature" would be a vulnerability.

Detecting Incidents

- Incidents may be detected by users or administration staff
  - Staff should be encouraged to make reports of system malfunctions or anomalous behaviors
- Automated tools
  - System integrity verification tools
  - Log analysis tools
  - Network and host intrusion detection systems (IDS)
  - Intrusion prevention systems

Triage Function



Goal:

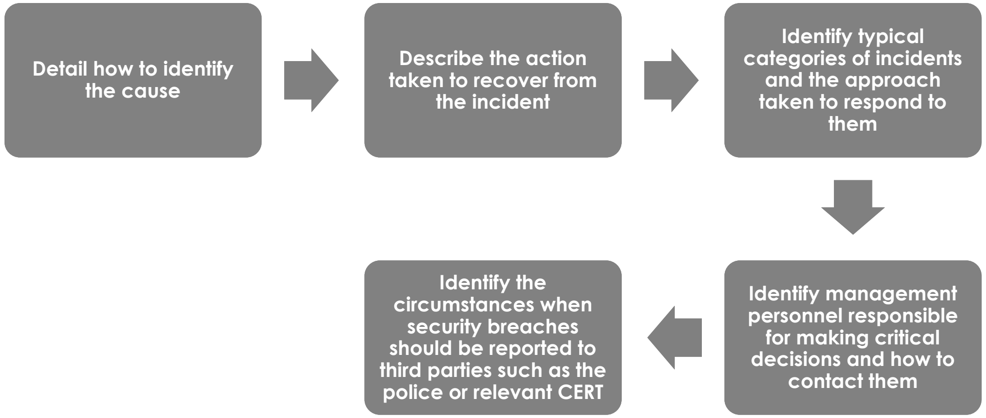
- Ensure that all information destined for the incident handling service is channeled through a single focal point
- Commonly achieved by advertising the triage function as the single point of contact for the whole incident handling service

Responds to incoming information by:

- Requesting additional information in order to categorize the incident
- Notifying the various parts of the enterprise or constituency about the vulnerability and shares information about how to fix or mitigate the vulnerability
- Identifies the incident as either new or part of an ongoing incident and passes this information on to the incident handling response function

Responding to Incidents

- Must have documented procedures to respond to incidents
- Procedures should:



Detail how to identify the cause

Describe the action taken to recover from the incident

Identify typical categories of incidents and the approach taken to respond to them

Identify management personnel responsible for making critical decisions and how to contact them

Identify the circumstances when security breaches should be reported to third parties such as the police or relevant CERT

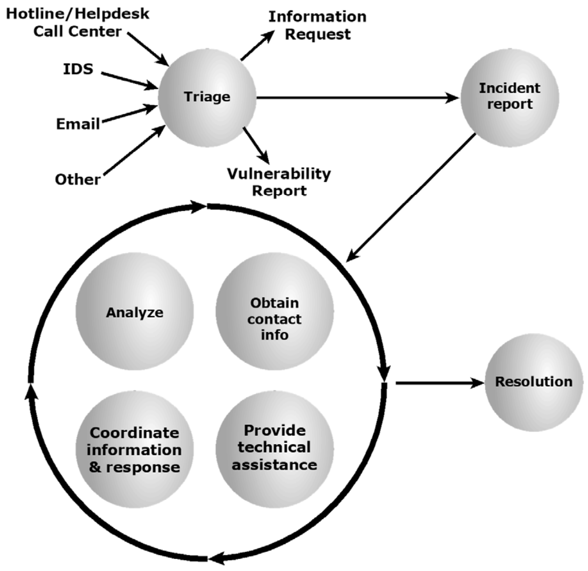
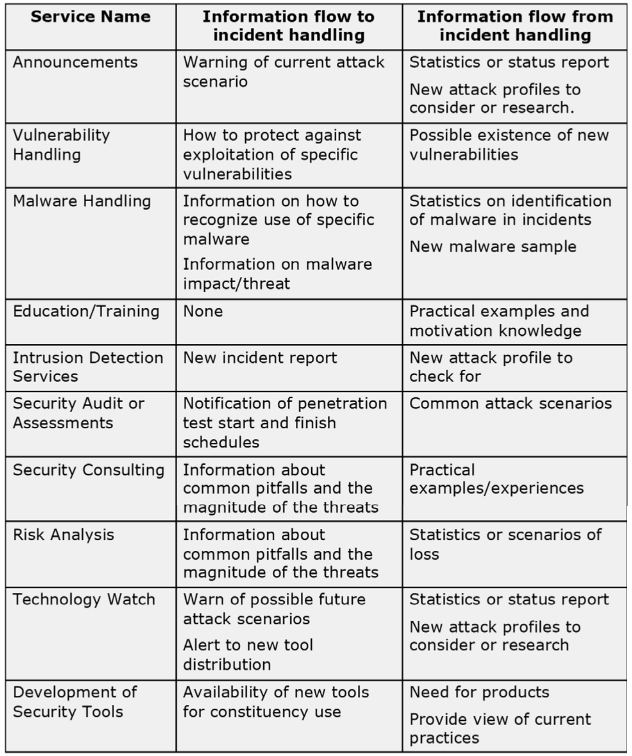


Figure 17.2 Incident Handling Life Cycle

Documenting Incidents

- Should immediately follow a response to an incident
  - Identify what vulnerability led to its occurrence
  - How this might be addressed to prevent the incident in the future
  - Details of the incident and the response taken
  - Impact on the organization’s systems and their risk profile



Service Name	Information flow to incident handling	Information flow from incident handling
Announcements	Warning of current attack scenario	Statistics or status report New attack profiles to consider or research.
Vulnerability Handling	How to protect against exploitation of specific vulnerabilities	Possible existence of new vulnerabilities
Malware Handling	Information on how to recognize use of specific malware Information on malware impact/threat	Statistics on identification of malware in incidents New malware sample
Education/Training	None	Practical examples and motivation knowledge
Intrusion Detection Services	New incident report	New attack profile to check for
Security Audit or Assessments	Notification of penetration test start and finish schedules	Common attack scenarios
Security Consulting	Information about common pitfalls and the magnitude of the threats	Practical examples/experiences
Risk Analysis	Information about common pitfalls and the magnitude of the threats	Statistics or scenarios of loss
Technology Watch	Warn of possible future attack scenarios Alert to new tool distribution	Statistics or status report New attack profiles to consider or research
Development of Security Tools	Availability of new tools for constituency use	Need for products Provide view of current practices

Table 17.3

Examples of Possible Information Flow to and from the Incident Handling Service

Summary

- Security awareness, training, and education
  - Motivation
  - A learning continuum
  - Awareness
  - Training
  - Education
- Employment practices and policies
  - Security in the hiring process
  - During employment
  - Termination of employment
- E-Mail and Internet use policies
  - Motivation
  - Policy issues
  - Guidelines for developing a policy
- Computer security incident response teams
  - Detecting incidents
  - Triage function
  - Responding to incidents
  - Documenting incidents
  - Information flow for incident handling