AL-FARABI KAZAKH NATIONAL UNIVERSITY

FACULTY OF INFORMATION TECHNOLOGY AND ARTIFICIAL INTELLIGENCE
DEPARTMENT OF CYBERSECURITY AND CRYPTOLOGY

LEGAL REGULATION OF INFORMATION SECURITY

Lecturer: PhD, Acting Associate Professor Assem Turarbek

MODULE 3

VIOLATIONS AND LEGAL LIABILITY

LECTURE 11

CLASSIFICATION OF INFORMATION SECURITY VIOLATIONS

LECTURE OBJECTIVE

Classify information security violations by actor, conduct, technical effect and legal regime.

LECTURE PLAN

1. Violations by actor and conduct

2. Impact on confidentiality, integrity and availability

3. Severity and legal classification

CLASSIFICATION BY RESPONSIBLE PARTY

Concept or participant	Meaning, duties and application
Owner or holder	May breach a duty associated with protecting, operating or testing the system.
User or administrator	May exceed assigned privileges or disregard use and operating rules.
External party	May attempt to access a system without permission.
Public authority	May exceed its competence, for example by imposing a requirement with no legal basis.

The actor’s role determines which duties and powers are relevant. Owners make organizational decisions, administrators exercise technical privileges, users act within service conditions and outside parties may have no permission to access the system. An authorized public body is also limited by its competence when imposing requirements.

ACTION AND OMISSION

Concept or participant	Meaning, duties and application
Action	A person carries out conduct that breaches an applicable rule, such as disclosing a restricted report.
Omission	A person fails to act when a duty requires action, such as neglecting an assigned review of access rights.
Assessment	Determine which duty applied and what the actor did or failed to do.

An omission requires a duty to perform the missing action. The assessment identifies who had that duty, when it applied and whether the person could perform it. Evidence may include work assignments, schedules and operating records. A prohibited action is assessed against the rule limiting what the actor was allowed to do.

IMPACT ON SECURITY PROPERTIES

Concept or participant	Meaning, duties and application
Confidentiality	Information is disclosed to someone without permission.
Integrity	Information is changed or destroyed without authorization.
Availability	Authorized people lose access to information or a service.

A single event can affect several properties. Disclosure affects confidentiality, an unauthorized change affects integrity, and an outage affects availability. The incident report records each observed effect. This technical classification describes the consequences for information, while the legal classification separately identifies applicable duties and possible responsibility.

CLASSIFICATION BY LEGAL REGIME

Civil

Infringement of private rights or failure to perform a contractual duty.

Disciplinary

Breach of duties within an employment relationship.

Administrative

Violation defined by administrative law.

Criminal

Conduct meeting the legal elements of a criminal offence.

The same technical behaviour may have different legal significance in different relationships. An employee’s use of an account can concern workplace duties and another person’s rights. An external intrusion raises other questions about permission and conduct. Each classification depends on the governing rule and the facts established.

ASSESSMENT OF CONSEQUENCES

Scale

Record how many systems, records and people were affected.

Severity

Consider service interruption, sensitivity of information and actual or potential harm.

Legal classification

Technical severity helps describe the incident. The applicable law and evidence determine legal qualification.

Severity concerns scope, sensitivity and service impact. The duration of an outage, the number of affected records and the consequences for users help describe harm. Legal qualification additionally depends on the applicable elements and evidence. Technical labels such as high severity do not by themselves establish a criminal offence.

CASE DISCUSSION

A system owner bypasses a required security test. Later, an administrator discloses a restricted report to a third party.

How would you classify each action by actor and affected security property?

Analysis

The owner’s act concerns an operating or testing duty. The administrator’s disclosure concerns a user with privileged access and affects confidentiality. Legal classification depends on the applicable duty and the evidence.

OWNER AND ADMINISTRATOR VIOLATIONS

An owner may fail to fulfil an organizational duty, such as arranging a required system test. An administrator may exceed privileges or disregard operating procedures.

The distinction helps identify the applicable duty and the evidence needed. A testing record concerns organizational compliance, while an access log can show how an administrator used technical permissions.

An external actor may attempt unauthorized access or interfere with a service. The assessment examines the relevant access boundaries and the conduct attributed to that actor.

A competent authority also operates within defined powers. The lecture gives an example of demanding documentation without a legal basis as a possible violation by an authorized body.

OMISSION REQUIRES AN ASSIGNED DUTY

An omission is legally relevant when the actor had a duty to act. Examples include a required access review or an assigned backup operation that was not performed.

The investigation identifies the source of the duty, the responsible person and the opportunity to perform it. Work assignments and operational records are therefore important evidence.

A single incident can affect more than one security property. Copying a dataset affects confidentiality, altering it affects integrity, and blocking the system affects availability.

The classification records each effect and each actor separately where appropriate. This prevents a broad incident label from obscuring different duties or distinct acts.

CONCLUSION

1. A violation can be classified by actor, by action or omission and by its technical effects.

2. Confidentiality, integrity and availability describe what was affected.

3. Legal classification depends on the applicable duty and the evidence.

SELF-ASSESSMENT QUESTIONS

1. How can security violations be classified by actor and conduct?
2. What distinguishes a violation caused by an action from one caused by an omission?
3. How can a single violation affect confidentiality, integrity and availability?
4. How does technical classification differ from legal classification?
5. What evidence is needed to connect a violation to a particular duty or prohibition?

REFERENCES

1. Lecture 11. Classification of Information Security Violations. Course materials.

2. ISO/IEC 27001 and ISO/IEC 27002. Information security management and controls.

3. T. R. Peltier. Information Security Policies, Procedures, and Standards.