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 4

INCIDENT RESPONSE AND INVESTIGATION

LECTURE 13

INFORMATION SECURITY INCIDENTS AND THEIR TYPES

LECTURE OBJECTIVE

Distinguish an event, an incident and an attack, and classify incidents by scope, effects and severity.

LECTURE PLAN

1. Events, incidents and attacks
2. Incident types and severity
3. Crisis assessment and escalation

EVENT, INCIDENT AND ATTACK

Concept or participant	Meaning, duties and application
Security event	An observable occurrence such as an unusual login, configuration change or service alert.
Information security incident	A failure or set of events that threatens normal operation or creates conditions for unauthorized actions involving digital resources.
Computer attack	A deliberate attempt to gain unauthorized access or interfere with an information resource or system.

An observable event becomes an incident when its facts meet the relevant incident criteria. An attack describes deliberate conduct aimed at unauthorized access or interference. Some attacks fail, and some incidents arise without deliberate action. Classification therefore begins with evidence of the event and its effects.

CLASSIFICATION BY FREQUENCY AND SCOPE

Concept or participant	Meaning, duties and application
Isolated or recurrent	One occurrence can be distinguished from repeated events over time.
Linked or widespread	Related events may form one incident. A mass incident affects multiple users or systems.
Affected object	The impact may concern one component, an entire system or a third-party dependency.

Frequency and relationship describe different features. Repeated events recur over time, while connected events share a cause or dependency. A widespread incident affects many systems or participants. Establishing a connection requires comparing accounts, timestamps, technical indicators and affected resources rather than relying only on similar symptoms.

CLASSIFICATION BY EFFECT AND TYPE

Concept or participant	Meaning, duties and application
Data effects	Unauthorized collection, copying, disclosure, modification or destruction.
Service effects	Blocking data access or interrupting the operation of a system or network.
Common categories	The lecture lists denial of service, malware, phishing, account compromise and unauthorized changes.

The type of incident helps select the investigation and response. A denial-of-service event primarily affects availability, while stolen credentials may lead to disclosure or alteration. Malware can create several effects at once. Recording the observed behaviour and the affected resource makes the classification more informative than a broad label alone.

SEVERITY SCALE IN THE LECTURE

Levels 0–1

White and green cover minor events or events with limited potential impact.

Level 2

Yellow covers probable disruption or adverse effects with a limited service impact.

Level 3

Orange covers possible significant restrictions or substantial consequences.

Levels 4–5

Red and black cover possible or imminent loss of service with serious effects.

The scale in the source combines likelihood or imminence with potential service consequences. Levels increase from white and green through yellow and orange to red and black. An assessment can change as the team learns that more systems are affected or that a threatened interruption is already occurring.

FROM INCIDENT TO CRISIS

Public services

A crisis can arise when an incident threatens access to public services.

Wider consequences

Effects on national security, the economy, infrastructure or population can justify crisis coordination.

Legal assessment

An incident assessment and an offence assessment use different criteria and evidence.

A crisis can extend beyond the owner of the affected system. Restrictions on public services or consequences for public safety and strategic infrastructure can require coordinated action. The assessment considers dependencies and potential spread. Operational teams then provide the information needed for decisions across participating organizations.

RECORDING AND TRIAGE

Initial facts

Record detection time, systems involved, observed effects and immediate actions.

Classification

Identify the incident type, scope and likely severity. Revise the assessment as evidence changes.

Escalation

Route the incident to the team responsible for containment and recovery.

Triage records what is known, what is uncertain and which actions have already been taken. A useful record includes detection time, affected assets, observed effects and the responsible team. Updates preserve the changing assessment. This history supports response handovers, recovery decisions and a later review of the incident.

CASE DISCUSSION

A public portal experiences repeated outages, and the monitoring team detects an unusual login.

What would you record, how would you judge severity, and what would justify treating the events as linked?

Analysis

Record service impact, duration, affected systems and the available login evidence. Treat events as linked only if their timing and other records support a common cause. Classification can change as evidence clarifies the scope and cause.

REPEATED AND INTERCONNECTED INCIDENTS

Repeated incidents recur over time. Interconnected incidents share a relationship, such as the same compromised account or common infrastructure. Widespread incidents affect many users or systems.

The response team tests the proposed connection against evidence. Similar symptoms alone may arise from different causes, while different symptoms can result from one underlying event.

An incident may affect an entire information system, one component or an auxiliary service. A third-party dependency can interrupt an organization even when its own application remains operational.

An impact assessment maps the affected dependency to the services that rely on it. This helps set recovery priorities and identify the organizations that need notification.

SEVERITY AND SERVICE CONSEQUENCES

The lecture’s six-level scale ranges from level 0, white, to level 5, black. Intermediate levels use green, yellow, orange and red to indicate increasing potential impact and urgency.

Severity considers the possibility of an event and its consequences for services and information resources. The assessment changes when new evidence shows a larger scope or more serious disruption.

Incident management establishes the technical facts and supports restoration. A legal assessment examines whether particular conduct meets the elements of an offence.

Some unlawful conduct can occur before a visible service incident. Other incidents arise from technical failure or human error. The evidence determines which further assessment is appropriate.

CONCLUSION

1. An alert is evidence of an event. Triage determines whether it represents an incident.

2. Severity reflects potential service impact and the wider consequences.

3. Classification can change as evidence clarifies the scope and cause.

SELF-ASSESSMENT QUESTIONS

1. How do an event, an alert, an incident and an attack differ?
2. What factors determine the severity of an incident?
3. How can investigators distinguish recurring incidents from connected events?
4. Why may an incident’s classification change during an investigation?
5. What information should be recorded when an incident is first reported?

REFERENCES

1. Lecture 13. Information Security Incidents and Their Types. Course materials.

2. ISO/IEC 27035. Information security incident management.

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