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 14

INCIDENT PREVENTION AND RESPONSE

LECTURE OBJECTIVE

Explain how preventive controls and response plans support detection, containment, recovery and coordination.

LECTURE PLAN

1. Prevention and response planning

2. Triage, containment and recovery

3. Crisis coordination and follow-up

PREVENTION AND READINESS

Concept or participant	Meaning, duties and application
Asset and risk review	Identify important systems, likely failure scenarios and the controls already in place.
Preventive controls	Use access controls, secure configurations, maintenance and monitoring to reduce exposure.
Continuity planning	Maintain backups, assign responsibilities and rehearse escalation and recovery.

Readiness depends on understanding assets and likely failure scenarios before an incident occurs. Preventive controls reduce exposure, while monitoring makes suspicious activity visible. Backups and continuity arrangements address disruption. Exercises test whether people know their roles and whether the planned communication and recovery steps work in practice.

INCIDENT RESPONSE PLAN

Concept or participant	Meaning, duties and application
Detection and notification	Define what staff report, who receives reports and when to escalate.
Containment and evidence	Describe measures to limit harm and preserve relevant logs, records and reports.
Recovery and review	Specify how services are restored, how restoration is checked and how recurring causes are addressed.

A response plan connects technical actions with responsibilities and communications. The source includes preservation of logs and reports, identification of causes, continuity measures and restoration. The plan also specifies interaction with operational and national coordination centres where applicable. The organization adapts these measures to its infrastructure and processes.

DETECTION, TRIAGE AND CONTAINMENT

Concept or participant	Meaning, duties and application
Detection	Validate the alert and record observed effects.
Triage	Estimate scope and urgency, identify the system owner and assign a response lead.
Containment	Restrict affected access or isolate affected components while keeping essential services available where possible.

Triage determines whether an alert represents an incident, which assets are affected and how urgent the response is. Containment then limits further harm. The chosen action considers essential services and evidence preservation. A record of decisions helps explain why a component was isolated, an account restricted or a service kept available.

EVIDENCE PRESERVATION AND RECOVERY

Preservation

Keep relevant records with timestamps and document how the team obtained and handled them.

Cause and remediation

Establish the likely cause and correct the conditions that allowed the incident.

Recovery

Restore from trusted resources, verify data integrity and monitor the service after restoration.

Recovery can change or remove information that explains the incident. Relevant logs, affected records and a handling history therefore support both diagnosis and later examination. Restoration uses trusted resources and includes integrity checks. Continued monitoring helps detect a remaining cause or a recurrence after the service returns.

COORDINATION IN KAZAKHSTAN

Owners and security centres

Owners manage response in their environments and work with operational centres.

National coordination centre

Consolidates information and supports communication among response participants.

Operational headquarters

Coordinates action across organizations when an incident becomes a crisis.

Local response and national coordination operate at different scopes. Owners and operational centres act in their environment and communicate findings. The national centre consolidates information across participants. A crisis headquarters coordinates broader action when the incident threatens several services or has wider consequences.

AFTER-ACTION REVIEW

Timeline

Record the sequence of events, decisions and communications.

Control review

Identify why prevention, detection or containment succeeded or failed.

Follow-up

Assign owners and deadlines for improvements and test the revised procedures.

The review reconstructs the event, examines which controls worked and identifies gaps in prevention or response. Each corrective action has an owner and completion criterion. A revised procedure or configuration also needs verification. Otherwise the record may show that an action was assigned without establishing that it reduced the risk.

CASE DISCUSSION

An electronic service is unavailable and multiple teams report conflicting information about the outage.

What should the response lead verify first, and what evidence should the teams preserve before recovery?

Analysis

Validate the outage and affected services, name a response lead and preserve event logs, timestamps and a decision record before restoration changes the environment. Recovery includes verifying service and data integrity and addressing the underlying cause.

CONTENTS OF A RESPONSE PLAN

The lecture lists prevention, collection and analysis of security information, coordination with operational centres, continuity arrangements and notification of affected participants.

The plan also covers preservation of digital traces, identification and removal of causes, follow-up actions and recovery. Defined responsibilities help staff use these procedures during a disruption.

The source describes an operational headquarters for coordination when an incident creates a security crisis. Before it convenes, primary response measures aim to limit spread and reduce consequences.

Its tasks include coordinating organizational and technical action, adjusting the actions of participating teams and organizing restoration and investigation.

CROSS-BORDER AND EMERGENCY COORDINATION

Incidents affecting organizations in several jurisdictions may require cooperation through authorized channels and applicable international arrangements.

During broader emergencies, communication and infrastructure management can involve additional competent bodies. Response plans therefore identify both ordinary contacts and escalation arrangements.

Restoring service addresses the immediate interruption. Removing the cause reduces the chance of another incident. Both activities require checks that the intended change has actually worked.

The after-action record links findings to assigned improvements. Examples include revised access controls, corrected configurations, improved monitoring and a new recovery test.

CONCLUSION

1. A response plan assigns roles and specifies notification, containment and restoration procedures.

2. Preserving evidence supports diagnosis and any subsequent investigation.

3. Recovery includes verifying service and data integrity and addressing the underlying cause.

SELF-ASSESSMENT QUESTIONS

1. What preventive measures reduce the likelihood of information security incidents?
2. What roles and procedures should an incident response plan define?
3. How do triage, containment and recovery differ?
4. Why is evidence preservation important during incident response?
5. How can lessons learned from an incident improve future security measures?

REFERENCES

1. Lecture 14. Incident Prevention and Response. Course materials.

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

3. NIST SP 800-61 Rev. 2. Computer Security Incident Handling Guide, as cited in the lecture.