Practical no:8

Name: Saloni Vishwakarma
Batch-Roll no: C1-13

Privileged and Confidential Attorney-Client Communication/Work Product

Date and Time of Notification: April 9, 2024, 3:15 PM	
Incident Detector's Information:	
Name: Emily Johnson	Date and Time Detected: April 9, 2024, 2:30 PM
Title: Network Administrator	Location: Data Center

Phone/Contact Info: 1234567890
System or Application: Financial Database

Type of Incident Detected:

☐ Denial of Service ■ Malicious Code ☐ Unauthorized Use ☐ Unauthorized Access ☐ Unplanned Downtime ☐ Other

Description of Incident: Suspicious file uploads were detected in the financial database system.
Names and Contact Information of Others Involved: N/A
☐ IS Leadership ☐ System or Application Owner ■ System or Application Vendor ■ Security Incident Response Team ☐ Public Affairs ■ Legal Counsel ☐ Administration ☐ Human Resources ☐ Other:
Identification Measures (Incident Verified, Assessed, Options Evaluated): Incident verified, assessed, and options evaluated.
Containment Measures:Access to the financial database was immediately restricted.
Evidence Collected (Systems Logs, etc.): Server logs and file upload history were collected for analysis.
Eradication Measures: Malicious files were identified and removed from the system

Recovery Measures: The financial database was restored from a clean backup.

Other Mitigation Actions: Enhanced firewall rules implemented to prevent future unauthorized uploads.

This form has been developed as a working tool for assessment and improvement activities; it is intended for internal use only. Journal of

Privileged and Confidential Attorney-Client Communication/Work Product

How Well Did Work Force Members Respond?
The response was swift and effective.

Were the Documented Procedures Followed? Were They Adequate?
Documented procedures were followed, but improvements are needed for proactive threat detection.

What Information Was Needed Sooner?
Real-time monitoring of file uploads would have expedited detection.

Were Any Steps or Actions Taken That Might Have Inhibited the Recovery?
No, all actions were taken to facilitate recovery without hindrance.

What Could Work Force Members Do Differently the Next Time an Incident Occurs?
Implement more stringent access controls to prevent unauthorized uploads.

What Corrective Actions Can Prevent Similar Incidents in the Future?
Regular security patching and vulnerability scanning.

What Additional Resources Are Needed to Detect, Analyze, and Mitigate Future Incidents?
Implementation of advanced threat detection software and employee training on cybersecurity best practices.

Other Conclusions or Recommendations:
Conduct a comprehensive review of all system access permissions.

Reviewed By:

☐ Security Officer ☐ IS Department/Team

☐ Privacy Officer ☐ Other

Recommended Actions Carried Out:
Enhanced firewall rules implemented, and staff training scheduled.

Initial Report Completed By:
Emily Johnson

Follow-Up Completed By:
Security Incident Response Team

This form has been developed as a working tool for assessment and improvement activities; it is intended for internal use only. 70 Journal of