

Privileged and Confidential Attorney-Client Communication/Work Product

Date and Time of Notification:	
Incident Detector's Information:	
Name:	Date and Time Detected:
Title:	Location:

Phone/Contact Info: System or Application:

Type of Incident Detected:

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

Description of Incident:
Names and Contact Information of Others Involved:
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):
Containment Measures:
Evidence Collected (Systems Logs, etc.):
Eradication Measures:
Recovery Measures:
Other Mitigation Actions:

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

AHIMA/January 2008 - 79/1 69

Privileged and Confidential Attorney-Client Communication/Work Product

How Well Did Work Force Members Respond?

Were the Documented Procedures Followed? Were They Adequate?

What Information Was Needed Sooner?

Were Any Steps or Actions Taken That Might Have Inhibited the Recovery?

What Could Work Force Members Do Differently the Next Time an Incident Occurs?

What Corrective Actions Can Prevent Similar Incidents in the Future?

What Additional Resources Are Needed to Detect, Analyze, and Mitigate Future Incidents?

Other Conclusions or Recommendations:

Reviewed By:

Security Officer IS Department/Team

Privacy Officer Other

Recommended Actions Carried Out:

Initial Report Completed By:

Follow-Up Completed By:

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

AHIMA/January 2008 - 79/1