**Cybersecurity incident report template**

*By Paul Kirvan, FBCI, CISA*

|  |
| --- |
| **Report Title:** Cybersecurity Incident Report |
| **Event Description:** |
| **Date of Event:** | **Time Event Identified:** |
| **Date Event Resolved:** | **Time Event Resolved:** |
| **Employees Participating in Event:** |
| **Describe how the event was initially detected.** |
| **What was the initial assessment of the event? Include data from security systems, firewalls, IDS/IPS, BAS systems, etc.** |
| **What technology systems, data, networks and other assets were affected?** |
| **Describe how the assets were affected by the event.** |
| **What was the impact of the event on the business and its operations?** |
| **Why did the attack occur? What caused the attack?** |
| **What steps were taken to contain the incident, quarantine it and analyze it to identify a remedy?** |
| **What were the results of the steps taken?** |
| **What alternate steps were taken, if the primary actions were unsuccessful?** |
| **What were the results of the alternate steps taken?** |
| **How did the company accommodate the event, recover and return to normal operations? How long did it take?** |
| **If the company was unable to quickly return to business following the event, what steps were needed for it to return to normal operations? How long did it take?** |
| **What preemptive steps could have been taken to prevent the event from occurring?** |
| **What recommended actions can be taken to prevent future occurrences?** |
| **What additional lessons were learned from the event?** |
| **Comments:** |
|  |
| **Originating Department:** IT Cybersecurity | **Version:** Original |
| **Prepared by:** | **Reviewed by:** |
| **Date Prepared:** | **Date Reviewed:**  |
| **Approved by:** | **Senior Management Approved by:** |
| **Date Approved:** | **Date Approved:** |
| **Release Date:** | **Date Updated:** |
|  |