**Delete This Page Before Creating Your Company’s Template**

**About This Document**

This Incident Progress Report (IPR) template is designed to guide organizations through the structured documentation and response process of cybersecurity incidents. It ensures critical steps are recorded, responsibilities are clear, and recovery efforts are effective. Whether dealing with a phishing attack, unauthorized access, or a data breach, this document provides a comprehensive framework to track progress from detection through resolution.

How to Use This Template

1. Start Immediately Upon Detection:
Begin documenting the incident as soon as it’s discovered. Record detection time, initial responders, and affected systems.
2. Update Regularly Throughout the Lifecycle:
As containment, investigation, and remediation progress, update the respective sections to ensure a clear timeline and accountability.
3. Use for Internal and External Communication:
The IPR can support communications with legal teams, regulatory bodies, clients, and insurance providers.
4. Leverage for Lessons Learned and Training:
Once closed, the report becomes a valuable resource for strengthening your security posture and preventing recurrence.

**About SpecGravity**

At SpecGravity, we specialize in simplifying technology operations for multiunit brands in hospitality, retail, and fast-scaling environments. Our cybersecurity services are built for agility and real-time protection, helping you navigate the complexities of today's threat landscape.

How We Help

* Immediate Incident Response:
Rapid containment, forensic investigation, and communication support when every minute counts.
* Prevention & Readiness:
We provide proactive solutions such as 24/7 monitoring, endpoint protection, vulnerability management, and employee training.
* Ongoing Support:
Through managed cybersecurity services, compliance guidance, and scalable solutions, we help you stay resilient and compliant long-term.

Need Help During or After an Incident?
Reach out to our cybersecurity team at:
📧 info@specgravity.com
📞 1-844-700-4728
🌐 [www.specgravity.com](http://www.specgravity.com)

**[Company Name] Cybersecurity Incident Progress Report (IPR)**

**Report Title**: e.g., Phishing Attack on Finance Team

**Report ID**: CS-INC-YYYYMMDD-XXX

**Date & Time Initiated**: YYYY-MM-DD HH:MM

**Reporter Name**: Full Name

**Contact Information**: Email / Phone

**1. Incident Overview**

* **Type of Incident**:
☐ Phishing
☐ Malware
☐ Unauthorized Access
☐ Denial of Service
☐ Data Breach
☐ Other: Specify
* **Date & Time Detected**: YYYY-MM-DD HH:MM
* **Detection Method**:
e.g., SIEM alert, employee report, antivirus alert
* **Systems/Assets Affected**:
e.g., Payroll Server, Email Gateway, Workstation #12
* **Impact Assessment**:
	+ ☐ Confidentiality
	+ ☐ Integrity
	+ ☐ Availability
	+ ☐ Financial Loss
	+ ☐ Compliance/Regulatory

**2. Incident Description**

**Detailed Description**:
Include what happened, how it was discovered, and any known or suspected cause.

**3. Initial Response**

* **Containment Measures Taken**:
e.g., isolated machine from network, reset passwords
* **Actions by Whom**:
e.g., IT Manager John Doe disabled affected accounts
* **Notifications Sent**:
☐ Internal IT/Security
☐ Legal/Compliance
☐ Affected Users
☐ Third Parties/Vendors
☐ Regulators

**4. Investigation Findings**

* **Root Cause Analysis**:
Summarize technical findings and vulnerabilities exploited
* **Indicators of Compromise (IOCs)**:
IP addresses, file hashes, domains, etc.
* **Log Review Summary**:
Mention any suspicious patterns or activities

**5. Remediation & Recovery**

* **Corrective Actions Taken**:
e.g., patched system, removed malware, enforced MFA
* **Recovery Steps**:
e.g., restored from backup, verified data integrity
* **Date/Time of Recovery**: YYYY-MM-DD HH:MM

**6. Communication Log**

| **Date/Time** | **Recipient/Team** | **Message Summary** | **Method (Email/Call/Meeting)** |
| --- | --- | --- | --- |
| YYYY-MM-DD HH:MM | e.g., Legal Team | Notified about potential data exposure | Email |

**7. Final Status & Lessons Learned**

* **Incident Status**:
☐ Closed
☐ Monitoring
☐ Escalated
☐ Ongoing Investigation
* **Key Lessons Learned**:
What went well, what can be improved, training gaps identified, etc.
* **Recommendations**:
e.g., stronger email filters, user awareness training

**8. Attachments**

* ☐ Screenshots / Logs
* ☐ System Reports
* ☐ External Communication Samples
* ☐ IOC Files
* ☐ Any Forensic Artifacts