GRC RISK REPORT

Case Study: Security Footage Data Destruction and Forensic Recovery (CTF Challenge**)**

Report ID: CTF2025-IMG-RECON

Date: 25 July 2025

Prepared by: Divyanshu Kumar

Confidentiality Level: Internal / Training

1. Executive Summary

This report documents a simulated breach scenario based on a Capture the Flag (CTF) challenge, where an attacker erased all security camera footage and logs, leaving only a network packet capture (.pcap) file as evidence. The exercise assessed the organization's forensic readiness, evidence recovery capabilities, and GRC (Governance, Risk, and Compliance) posture, with remediation strategies mapped to ISO/IEC 27001 and CERT-In guidelines.

2. Incident Description

- **a) Attack Vector:** Data destruction by an internal/external actor; only network packets (.pcap) remained post-attack.
- **b) Target:** Security camera system—video footage and logging infrastructure.
- **c) Impact:** Complete removal of standard video and log evidence. Recovery possible only through advanced packet and image carving.
- **d) Bypassed Controls:** Standard retention, backup mechanisms, and incident logging.

Forensic Steps & Recovery:

- Initial exploratory analysis using Wireshark to filter HTTP streams, identifying hundreds of JPEG fragments from an MJPEG video stream.
- Ineffective attempt at manual image recovery using binary/hex editors; shifted to automated file carving with **foremost**.
- Extraction of hundreds of JPEG images, each frame containing a flag character, requiring meticulous manual reassembly of the evidence.
- Ultimate recovery of the challenge "flag" demonstrated the importance of forensic tenacity and tool knowledge.

3. Risk Analysis

Attribute	Description
Asset at Risk	Security footage, forensic evidence, event trail
Threat Agent	Internal or external attacker (intent on destruction)
Vulnerability	Lack of tamper-proof evidence retention; no immutable backup; limited network anomaly detection
Impact (I)	High – Total loss of primary monitoring/audit trails
Likelihood (L)	Medium
Overall Risk	High (I x L)

4. ISO 27001 & CERT-In Control Mapping

Framework	Control Reference	Title/Requirement
ISO 27001	A.12.4	Logging and Monitoring
ISO 27001	A.8.16	Monitoring Activities
ISO 27001	A.5.23	Information Security Event Response
CERT-In	Section 2(e)	Mandatory incident reporting (within 6 hrs)
CERT-In	Section 4	Log retention for 180 days

5. Root Cause Analysis

- No encryption (HTTPS) used for streaming MJPEG data
- Surveillance system lacked data redundancy and offsite backup
- Poor logging practices — attacker's deletion not detected real-time
- No intrusion detection or packet anomaly alerts configured
- Security teams lacked readiness for packet-level forensic response

6. Remediation Plan

Action Item	Priority	Owner
Implement immutability and backup for logs/footage	High	IT Security
Deploy automated network packet anomaly detection	Medium	SOC
Regular forensic readiness and packet recovery drills	Medium	IR/Forensics
Update staff training for packet-level forensics	High	HR/Training
Integrate lessons learned into ISMS Risk Register	Medium	Compliance
Strengthen CERT-In reporting and evidence workflows	High	GRC Team

7. Policy & Compliance Recommendations

- Update **incident response policy** to require periodic testing and documentation of forensic recovery from raw packets.
- Mandate **quarterly forensic simulations** for staff, with CTF-style destructive event scenarios.
- Add data destruction and packet recovery scenarios to the **ISMS Risk Register**.
- Ensure all **CERT-In** reporting requirements are enforceable, tested, and evidence workflows are auditable.
- Enhance **backup, retention, and activity log policies** for tamper detection and offsite redundancy.

8. Conclusion

This simulated breach demonstrates that even when conventional audit trails are destroyed, well-trained teams with the right tools and patience can reconstruct evidence from network-level artifacts. It highlights the need for forensic readiness, advanced monitoring, robust backup, and continuous GRC alignment with ISO 27001 and CERT-In mandates.