FALCONE SYSTEMS

Cybersecurity Audit Report

March 1st 2024

Falcone Systems

200 First Avenue
Boston, Massachusetts 02116

Audit Company:
Knight Security

Table of Contents

Executive Summary

In March 2024, Knight Security conducted a comprehensive cybersecurity audit of Falcone Systems, focusing on evaluating the effectiveness and efficiency of the company's Media Protection controls. These controls are crucial for safeguarding information throughout its lifecycle, preventing unauthorized access, disclosure, alteration, and destruction.

The audit, grounded in the framework provided by NIST SP 800-53 and NIST SP 800-171 Rev. 2, assessed Falcone Systems' adherence to established media protection protocols through interviews, document reviews, and process testing.

The key findings in the audit were:

- **Lack of Formal Policies**: Absence of documented media protection policies and procedures, leading to inconsistent practices.
- **Effective Controls**: Proper media access and use controls are in place, including non-auto-mounting USBs, access control lists, and data loss prevention measures.
- **Partial Implementations**: Inconsistencies in media markings and sanitization documentation were noted, indicating a need for standardized procedures.
- **No Controls in Key Areas**: Missing controls for media storage and downgrading, posing significant security risks.

To close these gaps, Falcone Systems is advised to develop and implement comprehensive policies and procedures, standardize processes for media marking and sanitization, and introduce governance for media storage and downgrading. Implementation is recommended within 2 to 4 months, supported by regular compliance audits and a culture of continuous improvement.

Addressing these recommendations will strengthen Falcone Systems' defense against data breaches and align its practices with cybersecurity best practices.

Objective & Scope

The objective of this audit is to evaluate the effectiveness and efficiency of existing Media Protection controls at Falcone Systems. These controls are designed to safeguard information stored on both physical and electronic media throughout their lifecycle, preventing unauthorized access, disclosure, alteration, and destruction.

The audit included a review of Falcone's information security policies and processes in place during the FY of 2023.

Methodology

To fulfill the objectives of the audit, a third party Auditor, Knight Security implemented their audit program, to evaluate Falcone Systems' Media Protection controls based on the National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations. A template derived from NIST SP 800-171 Revision 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations served as the foundational framework for the audit process and was mapped to NIST SP 800-53 Media Protection (MP) controls.

Coordination with Falcone Systems facilitated onsite in-person interviews with two integral members of Falcone's IT team as shown in Fig. 1.

Job Title	Name	Date	Location
Director of IT	John Finnegan	23rd February 2024	Falcone Systems HQ
Network Engineer	Sam Cunningham	23rd February 2024	Falcone Systems HQ

(Fig. 1)

Preparation for the audit included the formulation of interview questions, tailored specifically to assess the Media Protection controls as per NIST SP 800-53. This was complemented by a request for critical documents, including Falcone IT Systems' Standard Operating Procedures and Security Plan, to be reviewed prior to the on-site interviews.

The on-site audit interview was conducted using tailored questions derived from NIST SP 800-53 Media Protections Controls, addressing both interviewees simultaneously. The primary goal of this audit phase were to:

1. Ensure comprehensive data collection during the interview.
2. Determine the implementation status of Media Protection controls.
3. Document evidence, noting both the provider and the nature of the evidence.
4. With the interviewees' consent, the session was both audio recorded and documented through notes.

Data collection encompassed interviews, document reviews, and testing to verify active implementation of processes.

For any additional information or to address pending action items, quick follow-up communications were promptly executed via email and phone following the audit interview.

The immediate goal following data collection was to compile and categorize the gathered information into an organized excel spreadsheet, adhering to specified column headings indicative of data type, evidence details, and findings. (See Fig. 2 for an example)

Data Collection	Evidence Detail	Findings
Interview	Director of IT	No controls in place
Tested	Network Engineer	Reviewed Documentation of Media Markings

(Fig. 2)

Data Collection Methodologies:

Category	Description
Interview	Conducted either through recorded Zoom meetings or in-person.
Documentation	Consists of documents provided by the interviewee.
Tested	Refers to processes currently in use and followed by the organization.

(Fig. 3)

Evidence Detail Types:

Type	Description
Person	The individual who provided the evidence.
Document/Process	A recorded document or an established process.

(Fig. 4)

Findings:

Type	Description
Information	Derived from the Evidence Detail.
Verification	All findings must be supported by factually verifiable evidence.

(Fig. 5)

Each piece of data—whether obtained through interviews, documentation, or testing—was recorded via audio recording or documented, ensuring that all findings are supported by factually verifiable evidence.

Audit Findings

The audit findings associated for each media protection control will be explained below.
A separate risk assessment report will outline the risks and vulnerabilities associated with these audit findings.

Each control is given a disposition value after data analysis as shown in Figure 6. The value meanings are self-explanatory.

Disposition	Value Meaning
Not in Place	Control is not in place
In Place	Control is in place and effective
Partially In Place	Control is not fully in place
N/A	Control is not necessary or required

(Fig. 6)

MP1: Policy and Procedures

Status: Not in Place.
Findings: Falcone Systems did not have any stored or documented media protection policy or procedure currently in place. The process was mostly undertaken by company ritual processes on an inconsistent basis by senior members of the IT department with some process written but not fully compiled.

MP2: Media Access

Status: In Place.
Findings: Falcone Systems USB drives are not auto mounted. All sensitive data is protected through access control lists and all database access is logged and tracked. A data loss prevention (DLP) process is also implemented blocking any data exfiltration of media files.

MP3: Media Markings

Status: Partially in Place.
Findings: Falcone Systems documentation of identified media for markings for Covid data and its financial data were inconsistent. All of Falcone Systems Covid data had markings however its financial data did not have consistent markings. This made it very confusing to attribute whether the financial data was highly sensitive or not.

MP4: Media Storage

Status: Not in Place.
Findings: No control or governance around thumb drive usage and storage were found to be in place at Falcone Systems including any documentation or training.

MP5: Media Transport

Status: In Place.
Findings: Falcone System's employees are prohibited from transporting company data during travel. Instead, the company utilizes cloud storage, enabling staff to access data directly from the cloud. Additionally, any system designated for maintenance or repair undergoes a thorough data wipe to remove sensitive information before being returned or discarded.

MP6: Media Sanitization

Status: Partially in Place.
Findings: Sanitization of media items is happening but inconsistently documented. Evidence detail showed reviewed last three audit records of HDD destroyed. One was recent, but the other two were three years old.

MP7: Media Use

Status: In Place.
Findings: There are no USB auto mounting allowed at Falcone Systems. All USB drives that are mounted are tracked and logged, and pre-approved within by an Access Control List. Only verified USB devices are allowed to mount otherwise the USB device is blocked and denied access.

MP8 Media Downgrading

Status: Not in place.
Findings: There are no documented processes for media downgrading of sensitive data.

A quick overview of the findings for each media protection control is shown in Figure 7.

Control Identifier	Control Name	Disposition
MP-1	Policy and Procedures	Not in Place
MP-2	Media Access	In Place
MP-3	Media Marking	Partially In Place
MP-4	Media Storage	Not in Place
MP-5	Media Transport	In Place
MP-6	Media Sanitization	Partially In Place
MP-7	Media Use	In Place
MP-8	Media Downgrading	Not in Place

(Fig. 7)

Recommendations

To address the audit findings and improve the media protection controls at Falcone Systems, the following mitigation strategies, along with realistic implementation timelines, are recommended for controls that are not in place or partially in place as shown in the Recommendation and Implementation Table (Fig. 8).

Recommendation & Implementation Table

Control ID	Recommendation	Implementation Timeline
MP1	Develop comprehensive media protection policies and procedures, including roles, guidelines, and consequences for non-compliance.	3 months for development. 1 month for implementation.
MP3	Standardize media marking procedures for all data types and conduct regular audits for compliance.	2 months to standardize procedures. Ongoing quarterly audits.
MP4	Establish policies for the usage and storage of removable media, focusing on encryption, physical security, and access control. Train employees on secure storage practices.	4 months total for policy development and training.
MP6	Standardize the media sanitization process with a verification mechanism. Train personnel on proper sanitization methods.	3 months for process development and training.
MP8	Develop a process for media downgrading that includes sanitization, declassification, and secure handling instructions. Train staff accordingly.	4 months for process development and staff training.

(Fig. 8)

Additional Notes:

- Quarterly Reviews: Implement quarterly reviews to assess policy compliance and the effectiveness of the implemented strategies. Adjust policies as necessary based on these reviews.
- Continuous Improvement: Foster a culture that prioritizes continuous improvement and adapts to technological and security changes. Update policies regularly to address new risks.

These strategies and timelines are designed to systematically address the gaps identified in the audit, ensuring that Falcone Systems enhances its media protection controls and complies with best practices in cybersecurity.

Appendices

Detailed Logs and Evidence: Interview transcripts and interview recordings, Falcone Standard Operating Procedures, Falcone Systems reviewed audit records.

Audit Team Members: Eric Chun.