FALCONE SYSTEMS

Cybersecurity Risk Assessment Report for Media Protection Controls

March 25th 2024

Falcone Systems

200 First Avenue
Boston, Massachusetts 02116

Report prepared by:
Knight Security

Table of Contents

Executive Summary

On March 2024, Knight Security performed an in-depth cybersecurity risk assessment of Falcone Systems' Media Protection controls, building on previous audit findings. Utilizing the NIST SP 800-30 Rev. 1 risk framework, the assessment aimed to evaluate the risks associated with partially implemented or absent media protection controls at Falcone Systems.

The assessment uncovered significant vulnerabilities stemming from the absence of formal policies and procedures, inconsistent media markings and sanitization documentation, and lacking controls for media storage and downgrading.

To address these issues, Knight Security recommended the development and enforcement of comprehensive policies and procedures, the standardization of media marking and sanitization processes, and the introduction of robust governance for media storage and downgrading. The recommendations suggest a timeline of up to 28 months for full implementation and integration, aiming to significantly bolster Falcone Systems' cybersecurity media protection posture.

Scope and Objectives

The risk assessment's scope was centered on evaluating media protection control, both non-existing and partially implemented, at Falcone Systems. These specific controls were identified based on insights derived from the recent 2024 Falcone Audit Media Controls Report findings.

The primary goal of this risk assessment is to assess the level of risk these media protection measures present to the organization and to develop strategies for their effective mitigation. Shown below are the media protection controls to be assessed.

Control Identifier	Name
MP-1	Policy and Procedures
MP-2	Media Access
MP-3	Media Marking
MP-4	Media Storage
MP-5	Media Transport
MP-6	Media Sanitization
MP-7	Media Use
MP-8	Media Downgrading

Methodology

In order to prepare for the risk assessment, we needed to identify the threats present first.

A modified threat list was compiled based of NIST SP 800-30 Appendix D and E.
Figure 1 below shows our modified threat list created.

Threat-Source	Threat	Description	Consequences
Human intentional/Human Unintentional	**Data modification/ destruction/ corruption**	An improperly protected system (e.g., unpatched or unprotected from malware) may allow data to be changed or destroyed.	Operational failure of Falcone Systems (loss of availability and integrity). Damaged / Falcone Systems reputation
Human intentional/Human Unintentional	**Damage/destruction of assets**	Destruction of the physical structure and IT assets will adversely affect the availability of a system.	Without infrastructure out of which to operate and without working IT assets, the systems supporting Falcone Systems will not be available.
Human intentional/Human Unintentional	**Data Loss/Information Disclosure**	An improperly protected system (e.g., unpatched or unprotected from malware) may allow for the intentional or inadvertent leakage of sensitive data.	Data loss may affect the ability of the Falcone Systems to meet its mission, but also open the up to litigation or result in serious damage to Falcone Systems reputation, including a costly response to any data leakage.
Human intentional/Human Unintentional	**Unauthorized access**	Access to systems and information which a person does not need can lead to data leakage or to the compromise of a system.	Operational failure of Falcone Systems (loss of availability and integrity) Damaged Falcone Systems reputation.

Human intentional/Human Unintentional	**Unauthorized changes to systems**	When changes are not tracked or authorized, system integrity and availability come into question.	Changes made to the system that are not tracked adversely affect the ability to recover from a disaster, rebuild a system, or recognize current vulnerabilities that may exist on a system due to its configuration.
Environmental/ Natural	**Temperature/humidity control**	Without adequate temperature or humidity control, IT systems may suffer adverse physical failures and affect availability.	If temperatures get too hot or too cold, equipment failures occur and systems will not be available.
Environmental/ Natural	**Power Failure**	Inadequate power will adversely affect the availability of a system.	Without adequate power and backup power, the systems supporting Falcone Systems will not be available.
Environmental/ Natural	**Fire**	Destruction of the physical structure and IT assets will adversely affect the availability of a system.	Without infrastructure out of which to operate and without working IT assets, the systems supporting Falcone Systems will not be available.
Environmental/ Natural	**Water damage**	Destruction of the physical structure and IT assets will adversely affect the availability of a system.	Without infrastructure out of which to operate and without working IT assets, the systems supporting Falcone Systems will not be available.
Environmental/ Natural	**Earthquake**	Destruction of the physical structure and IT assets will adversely affect the availability of a system.	Without infrastructure out of which to operate and without working IT assets, the systems supporting Falcone Systems will not be available.
Environmental/ Natural	**Typhoon**	Destruction of the physical structure and IT assets will adversely affect the availability of a system.	Without infrastructure out of which to operate and without working IT assets, the systems supporting Falcone Systems will not be available.

Environmental/ Natural	**Inability to recover from a disaster**	Without proper planning, resource support, and recovery documentation, Falcone Systems will be unable to recover from an event or disaster.	The inability to recover from a disaster can result in damage to Falcone Systems' reputation and the Falcone Systems' ability to support its mission.
Legal	**Policy breach**	The lack of policy or a violation of existing policy may open Falcone Systems up to other threats and vulnerabilities, such as data loss, unauthorized access, or other vulnerabilities.	The lack of policy or a violation of existing policy may open the Falcone Systems up to litigation or result in serious damage to the 's reputation
Managerial	**Lack of Resources**	Resources, including personnel and life cycle replacement of IT components, if not adequately put in place, can cause system failures or inability to provide adequate support to the Falcone Systems mission.	Without adequate resources, the Falcone Systems has suffered single points of failure which caused repeated repair or reinvention of processes.
Managerial	**Incomplete documentation**	Without an accurate inventory of managed systems within the Falcone Systems or maintenance information, security controls may not be effectively applied and subject the system to other vulnerabilities or exploits.	Undocumented systems may be used to exploit the Falcone Systems.

(Fig 1.)

Using the Threat value from the above table as inputs to add in an excel spreadsheet, we can start to add values with the following columns.

There are three new columns added into an excel spreadsheet with column names titled: `Threat(s)`, `Vulnerability Description` and `Mitigating Factors`. The excel spreadsheet is a continuation of the Falcone Systems Audit Report excel spreadsheet. This would make doing the risk assessment much easier.

The risk assessment file would have the following columns as shown in Figure 2. The Threats column was modified and referenced from Appendix Table E-2 Adversarial Threat Event from NIST SP 800-30.

Control Identifier	Threat(s)	Vulnerability Description	Mitigating Factors (Compensatory Controls)
MP-1			
MP-2			
MP-3			
MP-4			
MP-5			
MP-6			
MP-7			
MP-8			

(Fig. 2)

Now that we have entered our data for each threat, a description of the vulnerability and whether there was any mitigating factors for each control that was partially or not in place, we began to semi-quantify the risk by adding values for the likelihood and impact of each threat. We added another three columns titled: Likelihood, Impact and Risk Score.

Values that could be chosen were: 0, 2, 5, 8 and 10.

These values were referenced from NIST SP 800-30 Appendix G-2 and G-3 and Appendix H-3 tables, so we could accurately semi-quantify the Likelihood and Impact of each Vulnerability.

The Appendix Tables from NIST SP 800-30 that were referenced are shown below.

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the treat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event.

Table G-2: Assessment Scale – Likelihood of Threat Event Occurrence (Adversarial)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Error, accident, or act of nature is **almost certain** to occur; or occurs **more than 100 times a year**.
High	80-95	8	Error, accident, or act of nature is **highly likely** to occur; or occurs **between 10-100 times a year**.
Moderate	21-79	5	Error, accident, or act of nature is **somewhat likely** to occur; or occurs **between 1-10 times a year**.
Low	5-20	2	Error, accident, or act of nature is **unlikely** to occur; or occurs **less than once a year**, but **more than once every 10 years**.
Very Low	0-4	0	Error, accident, or act of nature is **highly unlikely** to occur; or occurs **less than once every 10 years**.

Table G-3: Assessment Scale – Likelihood of Threat Event Occurrence (Non-adversarial)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	21-79	5	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	5-20	2	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

Table Appendix H-3 Assessment Scale – Impact of Threat Events

Our Excel would look like this now as shown in Figure 3.

Control Identifier	Threat(s)	Vulnerability Description	Mitigating Factors (Compensatory Controls)	Likelihood	Impact	Overall Risk
MP-1						
MP-2						
MP-3						
MP-4						
MP-5						
MP-6						
MP-7						
MP-8						

(Fig. 3)

The next step is to calculate the Overall Risk. This value is calculated by multiplying the Likelihood value with the Impact Value. How the risk was evaluated is explained in the Risk Evaluation section of this report.

A final Risk Explanation column is added to explain what the risk would entail for Falcone Systems if the vulnerability was to be exploited. See Figure 4. This table was referenced and modified from Appendix I-5 Template – Adversarial Risk from NIST SP 800-30.

Control Identifier	Threat(s)	Vulnerability Description	Mitigating Factors (Compensatory Controls)	Likelihood	Impact	Overall Risk	Risk Explanation
MP-1							
MP-2							
MP-3							
MP-4							
MP-5							
MP-6							
MP-7							
MP-8							

(Fig. 4)

Threat and Vulnerability Analysis

The data presented in Figure 5 (Fig.5) reveals insights into Falcone Systems' risk management practices concerning its media protection controls. It outlines the various threats, vulnerabilities, and mitigating factors associated with the handling of media and information for each control identifier marked MP-1 to MP-8. Below is an analysis based on each control that is not fully in place. (MP2, MP5, MP7 is not analyzed).

MP-1 Policy and Procedures (Unauthorized Access)

The primary vulnerability is the absence of documented processes or policies, which opens the door to unauthorized access. The reliance on tribal knowledge (unwritten knowledge shared informally) as a compensatory control is insufficient and risky because it lacks formalization and consistency, making the organization highly susceptible to oversight and errors, especially with staff turnover.

MP-3 Media Marking (Data Loss/Information Disclosure)

This control highlights a vulnerability where financial data could be disseminated to unauthorized parties due to the absence of media marking. With no mitigating factors listed, this presents a clear risk of sensitive information leakage, emphasizing the need for implementation of marking protocols to prevent unauthorized access or disclosure.

MP-4 Media Storage (Data Loss/Information Disclosure)

There is a risk of introducing malware into the environment and the potential internal theft of data to Falcone Systems with this control. Even though Falcone Systems has implemented compensatory controls such as disabling auto-mounts for USB drives reducing the likelihood of malware infection through external media and unauthorized data extraction, it does not completely eliminate them.

MP-6 Media Sanitization (Data Loss/Information Disclosure)

This control points to the risk associated with inadequate record keeping for media sanitization, potentially leading to improper handling or loss of sensitive data. The mitigating factor relies on tribal knowledge and a small IT team. While potentially effective in a small organization, this poses scalability and reliability issues. Dependence on a single employee for consistent execution is a significant vulnerability due to the risk of personnel change, personnel absence or error.

MP-8 Media Downgrading (Data Loss/Information Disclosure)

This control identifies a vulnerability where highly sensitive or confidential information could be accidentally exposed to the public. The absence of mitigating factors indicates a critical gap in the organization's risk management practices, requiring immediate attention to implement controls to protect against inadvertent disclosure.

Control Identifier	Threat(s)	Vulnerability Description	Mitigating Factors (Compensatory Controls)
MP-1	Unauthorized Access	No documented processes or policies.	Tribal knowledge in place
MP-2	N/A	N/A	Control in Place
MP-3	Data Loss/ Information Disclosure	Without media marking, financial data could be disseminated to unauthorized parties. Financial data could accidentally be disseminated to unauthorized parties	None
MP-4	Data Loss/ Information Disclosure	Malware could be brought into the environment and inside threat could steal data.	USB Drive auto mounts disabled.
MP-5	N/A	N/A	Control in Place
MP-6	Data Loss/ Information Disclosure	Without record keeping there is no assurance of proper sanitization. New people could take over process and result in it not being done.	Tribal knowledge process and small IT team with one employee stating he consistently does it.
MP-7	N/A	N/A	Control in Place
MP-8	Data Loss/ Information Disclosure	Highly sensitive or confidential information could be accidentally exposed to the public.	None

(Fig. 5)

Risk Evaluation

A semi-quantitative approach was used to evaluate the risk of each vulnerability. Risk evaluation was referenced from NIST SP 800-30 Table I-3 Assessment scale.

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	**Very high risk** means that a threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	**High risk** means that a threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	**Moderate risk** means that a threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	**Low risk** means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	**Very low risk** means that a threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Table Appendix I-3 Assessment Scale – Level of Risk

A Likelihood versus Impact risk matrix is shown in Figure 6 to quantify and evaluate each risk.

- Values with a score >= 80 are high risk. This risk is extremely serious and must be remediated immediately (marked in red).
- Values with a score > 20 and < 80 are moderate risk. This risk can become more even serious and could have a negative effect on the company now so it should be remediated as soon as they can (marked in yellow).
- Values with a score of <= 20 are low risk and can be remediated accordingly (marked in green).

			Impact			
Likelihood	**0**	**2**	**5**	**8**	**10**	Risk Legend
10	0	20	50	80	100	High
8	0	16	40	64	80	Moderate
5	0	10	25	40	50	Low
2	0	4	10	16	20	
0	0	0	0	0	0	

(Fig. 6)

Below in Figure 7 shows the risk findings of each media control sorted by highest to lowest overall risk for Falcone Systems with a short risk explanation.

Here are the key risk findings:

- MP-8 has the highest overall risk to Falcone Systems especially regarding its handling of confidential data. This could pose a very serious threat to the company if exposed.
- MP-1 and MP-4 shows moderate risk regarding policy and protocols handling media protection, storage and sanitization and protecting stored media both digital and physical.
- MP-3 and MP-6 shows low risk as the likelihood of the event is low.

Control Identifier	Likelihood	Impact	Overall Risk	Risk Explanation
MP-8	8	8	64	If confidential digital information was accidentally exposed, such as proprietary information, trade secrets, and patents and so on, the negative impact would be severe and could cripple the business.
MP-1	5	5	25	Staff do not know what expectations or standards are and no process around media protection, storage, sanitization is documented so may not be done properly Without standards and policy no process can be repeated consistently and staff will develop their own individual processes.
MP-4	5	5	25	Loss of IP and introduction of malicious USB could introduce massive issues.
MP-3	2	8	16	Financial data isn't disclosed often by accident, but when it is it has a negative impact on moral and investor confidence.
MP-6	2	8	16	There is no assurance of proper sanitization. Tribal knowledge process. A new person may not know, and if theft occurred there would be no assurance of controlled data.
MP-2	0	0	0	Control in place
MP-5	0	0	0	Control in place
MP-7	0	0	0	Control in place

(Fig. 7)

Recommendations

Falcone Systems shows a mix of adequately managed controls and significant vulnerabilities, particularly in areas lacking formalized processes (MP-1, MP-3, MP-6, and MP-8). Below are the recommendations that can be implemented. These are sorted by highest to lowest risk.

MP-8 Media Downgrading (Risk Score: 64 – High Risk)

Goal:

- Enhance protection of confidential/sensitive information.

Methods:

- **Implement Strong Encryption:** Use encryption for all confidential digital information to ensure it's protected both at rest and in transit.
- **Data Masking**: Using a data masking protocol to hide or even completely redact sensitive or confidential information
- **Secure Deletion**: For physical media controls such as shredding, degaussing or destruction can be used and for stored digital media data can be completely wiped several times making it unrecoverable.
- **Clear Labeling and Documentation**: Downgraded media should be classified into a classification level and documented. Information would include the person who performed the downgrading, methods used, and dates for tracking purposes.
- **Auditing and Logging**: A log of all media downgrading activities should be maintained including what media is being downgraded, who performed the downgrade and methods used. Regular audits of this process should be maintained every quarter to ensure compliance.
- **Strict Access Controls:** Establish rigorous access controls, limiting sensitive data access to authorized personnel only, based on the principle of least privilege.
- **Training and Awareness:** Provide training for all individuals involved in the media downgrading process. This is includes understanding and following the necessary processes and protocols.

MP-1 Policy and Procedures (Risk Score: 25 – Moderate Risk)

Goal:

- Establish Clear Policies and Training.

Methods:

- **Document Policies and Processes**: Develop comprehensive, documented policies and procedures around media protection, storage, and sanitization.
- **Regular Training Programs**: Implement ongoing training programs for staff, focusing on adherence to these policies and best practices in media handling.

MP-4 Media Storage (Risk Score: 25 – Moderate Risk)

Goal:

- Secure Intellectual Property and Prevent Malware Risks

Methods:

- **Data Loss Prevention (DLP) Solutions:** Deploy DLP solutions to monitor and prevent the unauthorized sharing of intellectual property.
- **USB Drive Security:** Implement controls such as disabling auto-run features for USB drives and enforcing the use of approved, secure USB devices only.
- **Logging and Monitoring:** Log all approved USB drives logged into the organization's system and create alerts any non-approved USB drives. Pre-approve only acceptable software/programs run through the USB.

MP-3 Media Marking (Risk Score: 16 – Low Risk)

Goal:

- Safeguard Financial Data

Methods:

- **Data Handling Protocols**: Introduce secure handling and transfer protocols for financial data to prevent accidental disclosures.
- **Awareness and Training**: Enhance awareness programs focused on the importance of protecting financial information and the potential impacts of its disclosure.

MP-6 Media Sanitization (Risk Score: 16 – Low Risk)

Goal:

- Ensure Proper Media Sanitization

Methods:

- **Formalize Sanitization Processes:** Establish and document standardized processes for media sanitization to ensure all data is appropriately destroyed or wiped.
- **Audit and Accountability**: Introduce regular audits of sanitization practices and maintain logs to ensure compliance and accountability.

These recommendations will help prioritize addressing the most critical vulnerabilities first, ensuring that efforts and resources are allocated effectively to mitigate the highest risks to Falcone Systems.

Implementation Plan

The implementation plan for media controls is designed to enhance the security and management of media across various risk levels, including high, moderate, and low risks. The plan is structured around specific control identifiers (MP-8, MP-1, MP-4, MP-3, and MP-6) that address different aspects of media handling, including downgrading, policy and procedures, storage, marking, and sanitization. The duration of completing the implementation plan is expected to be around 28 months. The duration can always be adjusted accordingly. See figure 8 for the implementation plan timeline.

For high-risk areas under MP-8, the implementation plan outlines a series of actions that includes:

- Implementation of strong encryption
- Data masking
- Secure deletion (which includes both physical and digital media)
- Clear labeling and documentation
- Auditing and logging (with quarterly audits set up)
- Strict access controls
- Training and awareness programs

Moderate risk controls under MP-1 and MP-4 will focus on:

- Documenting policies and processes,
- Implementing regular training programs (with ongoing training after setup)
- Deploying Data Loss Prevention (DLP) solutions, enhancing USB drive security
- Setting up logging and monitoring to alert for non-approved USB drives

For low-risk areas, MP-3 and MP-6 emphasize:

- Introducing data handling protocols
- Enhancing awareness and training (ongoing after setup)
- Formalizing sanitization processes, and
- Establishing audit and accountability mechanisms.

Overall, the implementation plan is comprehensive, covering a broad range of media-related security measures aimed at mitigating risks and ensuring the safe handling and storage of media within the organization.

Control Identifier	Task	Start Month	Duration (Months)	End (Month)	Notes
MP-8 Media Downgrading (High Risk)	Implement Strong Encryption	1	2	2	
	Data Masking	3	2	4	
	Secure Deletion	5	1	5	Includes both physical and digital media
	Clear Labeling and Documentation	6	1	6	
	Auditing and Logging	7	1	7	Set up quarterly audits
	Strict Access Controls	8	2	9	
	Training and Awareness	10	2	11	Ongoing after initial setup
MP-1 Policy and Procedures (Moderate Risk)	Document Policies and Processes	12	2	13	
	Implement Regular Training Programs	14	1	14	Ongoing after initial setup
MP-4 Media Storage (Moderate Risk)	Deploy DLP Solutions	15	3	17	
	USB Drive Security	18	2	19	
	Logging and Monitoring	20	2	21	Implement alerts for non-approved USB drives
MP-3 Media Marking (Low Risk)	Introduce Data Handling Protocols	22	2	23	

	Enhance Awareness and Training	24	1	24	Ongoing after initial setup
MP-6 Media Sanitization (Low Risk)	Formalize Sanitization Processes	25	2	26	
	Audit and Accountability	27	2	28	

(Fig. 8)

Conclusion

The cybersecurity risk assessment of Falcone Systems highlighted crucial vulnerabilities within the company's media protection controls. Significant risks were identified in areas lacking formalized processes, including policy and procedure documentation, media marking, and sanitization practices, as well as media storage and downgrading controls. Addressing these vulnerabilities is critical for safeguarding Falcone Systems' information throughout its lifecycle, ensuring it remains protected against unauthorized access, disclosure, alteration, and destruction.

The proposed recommendations and subsequent implementation plan, aim to address these vulnerabilities by enhancing the security and management of media across various risk levels. Falcone Systems can significantly improve its cybersecurity posture, mitigating the risks associated with the handling and storage of media through the implementation of these recommendations.

Appendices

- Detailed Logs and Evidence: Supporting Audit documents & Risk Assessment Spreadsheet documents.
- Risk Assessment Team Members: Eric Chun.

References

- NIST SP 800-30 Guide for Conducting Risk Assessments Appendix Tables:
  E-2, G-2, G-3, H-2, I-3