ISEC-655 Fall 2022

Dr. Michelle Ramim

Eric Webb

Assignment #2 Executive Summary

November 27th, 2022

Dear Executives,

I have been tasked with conducting a formal review of the organizations device sanitation policy. Please see my detailed narrative below for basing future decisions on this subject matter.

Thank you again.

-Eric Webb

(CISSP)

**Old Computer and Device Sanitation Policy.**

1. Provide an overview of a small, medium, or large business that you are familiar with

The company is a very large and well-respected company. Currently there is a sanitation policy loosely enforced and defined. New hires are seeing old worker accounts on their laptops. The machines are not being sanitized properly. The policies defined state that machines should be properly sanitized before giving to the new hires, but no procedure is concretely defined.

2. Define the current state of Old Computer and Device Sanitation Policy.

Current state is a CMM3: *Senior Management and information security management have determined the levels of risk that an organization will tolerate and have standard measures for risk/return ratios. (Brotby, 2009)*

If they begin to enforce and manage old computer and devices sanitation properly. They could become a CMM4*: Responsibilities for information security are clearly assigned, managed and enforced. (Brotby, 2009)*

3. Select one of the approaches that we learned about including:

3.1. Indicate which approach you have selected and provide a brief logical support for your selection

The Capability Maturity Model gives an evolutionary path of increasingly organized and systematically more mature processes. It is used to develop and refine the security development process.

3.2. Complete an analysis for each element, attribute, and characteristic using the framework to determine the gap between the current state and the desired state related to the policy area selected.

Old computer and devices sanitation responsibility must be defined for all employees and contractors. Effort needs to be made to prevent old accounts from not being sanitized.

Accountability needs to be established.

3.3. Describe the unmitigated risk(s) from the current policy, and what it will require to “fill” the gap. Specifically, will it require different processes, technologies, controls, and so on to address the unmitigated risk(s)

There are a few unmitigated risks from the previous accounts not being properly sanitized.

*A- It exposes residual data of companies past endeavors.*

*B- Backdoor could have been left by previous worker.*

*C- New worker could use old account to masquerade.*

To fill the gaps, policies and procedures must be enforced to properly sanitize devices and hold accountability to the workforce.

3.4. Define the desired information security governance objectives and outcomes.

Management should have defined job responsibilities and procedure ownership for the IT sanitation team. All personnel should be aware of the responsibilities and ownership of assets and services that manages old computer and devices sanitation. Residual accounts should not be on new hire laptops.

Strategic Alignment – *Devices must be properly sanitized before reuse.*

Risk Management –R*esidual risk that needs to be addressed.*

Business Process Assurance and Convergence – *Verify from the top down that these policies and procedures are being established.*

Value Delivery – *Small investment for large risk relief.*

Resource Management – *Implement procedure checklist and peer review system with resources already available within the company to verify devices have been sanitized.*

3.5. Define the desired security risk management objectives and outcomes. (Hint: list

in chapter 8, p. 78)

1: The sanitization of devices has a standard procedure and any exception to the procedure

should be noticed.

2: Device sanitization has a defined management function with senior responsibility.

3: Senior management and IT security management have determined with metrics the levels of risk associated with device sanitization.

4: Responsibilities of device sanitization are clearly assigned, managed, and enforced.

5: Device sanitization risk and analysis is periodically performed.

6: Device sanitization procedures are performed at par or better with industry standards.

7: Periodic briefings on device sanitization.

8: Identification, authorization, and authentication are established before sanitization can occur.

9: Certifications are established and achieved for employee to sanitize device.

10: 3rd party audit is performed to verify sanitization.

11: Cost-Benefit analysis supporting the use of device sanitization are being utilized.

12: Sanitization processes coordinate with overall IT and organization processes.

13: Sanitization reports are linked to organization objectives.

14: Responsibilities and standards for device sanitization are constantly enforced.

15: The policies and practices of sanitization must be redundant with no single point of failure.

3.6. Suggest the time recovery objectives associated with the plan that you are

proposing to address the unmitigated risk(s). (Hint: p. 78)

The time recovery objectives associated with this plan is to decrease downtime risk with minimal investment in resources. By establishing and enforcing sanitization procedures the company mitigates risks that could lead to disaster. This positively effects the business impact analysis and disaster recovery time planning with little investment and big returns on mitigated risk.

3.7. Develop an information security strategy or suggest how to adjust the existing

security strategy related to the area that you selected (Hint: p. 90)

**Requirements:**

Devices need to be properly sanitized from previous users before lending to new user.

**Feasibility:**

Very feasible and relatively cheap operation costs.

**Design:**

Policies and procedures in place to sanitize both hard and soft data of device.

Proper accountability of sanitization with checklists and peer reviews.

Technical implementation of sanitization via cryptographic or data erasure.

Periodic briefings on data sanitization.

Metrics of devices being sanitized properly.

**Proof of Concept:**

Take a single device, sanitize it with new policy and procedures, get it peer reviewed, then audit it to see if it is truly sanitized.

**Development:**

Establish and document new policies and accountabilities.

Establish and document agreed upon procedures checklist and peer-review.

Establish chosen sanitization technique.

Establish and document metrics for sanitization results.

**Integration:**

Verify employees can sanitize a device properly and follow policies and procedures.

**Deployment:**

Roll out new policies and procedures company wide.

**Quality Testing:**

Get third party audit on sanitized device.

**Maintenance:**

Maintain software licensing if needed for sanitization, maintain briefings, and audits.

**Systems End of Life:**

Establish a replacement before end of life. Make sure this process is replicable and redundant.

3.8. Suggest an implementation plan, list the resources needed, and a plan on how to

gather support from the board of directions/senior management.

My plan on how to gather support from the board of directors is to explain to them the potential impact this can have on an organization compared to the relatively cheap solution for the problem. This can be done with industry examples where backdoors have been left on company machines that were not properly sanitized.

Resources Needed:

* Written policy of how to handle device sanitization.
* Written procedures of handling device sanitization.
* X employees dedicated to this task.
* X devices capable of performing sanitization.
* X software package licensing for sanitization.
* X trainings for sanitization.

3.9. Suggest a metric and monitoring process as well as compliance (Hint: p. 90)

A good metric is to send out a company surveys to employees asking them if their current devices have an old account on it. The same survey would be sent out to new hires after the processes have been implemented to see if their devices have not been sanitized.

Another metric is to look at the devices being turned in for sanitization. If they have more than one account tied to them then they were not properly sanitized before the last user.

3.10. Provide your opinion about the potential challenges with the executive

board as well as the implementation/compliance strategies. Are the objectives

realistic and achievable? Are the objectives likely to achieve the desired

outcomes? Predict the chances of success.

Dear Executives,

It is my opinion that maintaining an old computer and device sanitization policy can be quite difficult given the scale of the company, and I believe with a little adjustment success can be very realistic and achievable with little cost. This can be done through effective policy and procedures, accountability, proper training, and the correct tools. The objectives mentioned above are very likely to obtain their desired outcomes and I predict the chances of success to be very high. I would suggest implementing a stronger sanitization policy effective immediately.

Thank you again,

-ERIC WEBB

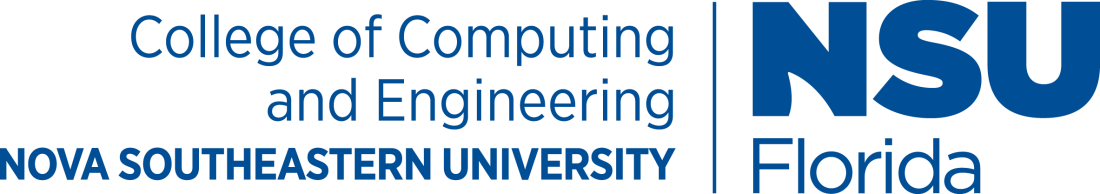
(CISSP)

# References

Brotby, K. (2009). Information security governance (1st ed.). John Wiley & Sons, Inc.

Amiri, A. (2007). Dare to share: Protecting sensitive knowledge with data sanitization. *Decision Support Systems*, pp*.* 181-191.

**Certification of Authorship of Doctoral Course Assignment**



Submitted to: Dr. Ramim

Student’s Name: Eric Webb

Date of Submission: November 27th, 2022

Purpose and Title of Submission: Assignment #2 Executive Review

Certification of Authorship: I hereby certify that I am the author of this document and that any assistance I received in its preparation is fully acknowledged and disclosed in the document. I have also cited all sources from which I obtained data, ideas, or words that are copied directly or paraphrased in the document. Sources are properly credited according to accepted standards for professional publications. I also certify that this paper was prepared by me for this purpose.

Student's Signature: ERIC WEBB