Yair Levy, Ph.D.

**ISEC 690  
Fall 2020  
Nova Southeastern University  
October 2020**

A Network hardening and data breach mitigation of an audio engineering studio

**Babatunde Somade and Eric Webb Figgy Z. (Owner), XYZ Audio Information Security Graduate Project**

Table of Contents

Executive Summary1

[Organizational Facts](#_Toc50574532) 2

[Project Scope and Goals 3](#_Toc50574533)

[Recommended Action Plan](#_Toc50574534) 4

[Network Topology](#_Toc50574535) 5

[Risk Management Analysis (RMA) 6](#_Toc50574536)

[Anticipated Results 7](#_Toc50574537)

[Proposed Costs 8](#_Toc50574538)

[Conclusion 8](#_Toc50574539)

[Reference 9](#_Toc50574539)

Executive Summary

Today’s business world lives off the production and manipulation of proprietary data, when information is the main product, it is imperative that it is kept safe (Leyshon, 2014). While keeping the product as secured as possible, businesses must still align themselves with best practices to mitigate risk (Jordan, 2012). Exposing company data or leaving it vulnerable to a breach could lead to a catastrophic business impact while simultaneously daunting the company's reputation. Loss of revenue and damage to reputation are some of the effects of a security breach. Gone are the days were small business were overlooked by bad actors, in fact, small business generates twice as much innovations and have more intellectual property than larger organization (Bhattacharya, 2015).

For many audio engineering studio's, digital attacks are a serious risk (Leyshon, 2014). Many clients within these organizations depend on the security and privacy of their projects to be successful. Most audio studios are small businesses with limited resources, no dedicated skilled information technology (IT) staff, and basic to no security features (Bhattacharya, 2015). When compared to large businesses that have dedicated security teams, audio studios are more suspectable to data theft and network intrusion (Bhattacharya, 2015).

This project will propose a more robust security posture for an audio engineering company, with a focus on network security through newer technology and best practices. This proposal will cover the current network topology and the proposed remediation for this audio engineering studio. The topics covered includes the Local Area Network (LAN), Data storage (transit and at rest), along with a malware and vulnerability assessment to determine risk. By following the principle of layered security and defense in depth (Jordan, 2012), the proposed solution will ensure Confidentiality, Integrity, and Availability of the business network infrastructure and intellectual property.

Organizational Facts

National Institute of Standards and Technology (NIST) recommends ways to remediate common vulnerabilities that could be easily exploited by bad actors. To follow this framework, initial audit was conducted at the Audio studio to identify current vulnerabilities that could be exploited and propose a plan to remediate them.

Physical Security Issues

* Studio doors do not have locks on them. Office building door has lock but once in, a perpetrator has access to recording equipment.
* Production computer should be locked away. Guest/Customers should not have physical access to them.
* No Security system in place to keep a record of access to the facility.

Network Security Issues

* Business has a flat network for all traffic. Production network is the same as guest network, no segregation.
* Guest connected to the WiFi can access the routers configuration.
* Business uses WiFi Protected Access (WPA) for security.
* Business does not use a Virtual Private Network (VPN) or Proxy.
* No network firewall, Intrusion Detection System (IDS), or Intrusion Prevention System (IPS).

Computer Security issues

* Production computer does not encrypt proprietary data on its local machine.
* Ports and Drives are not locked down from external hardware.

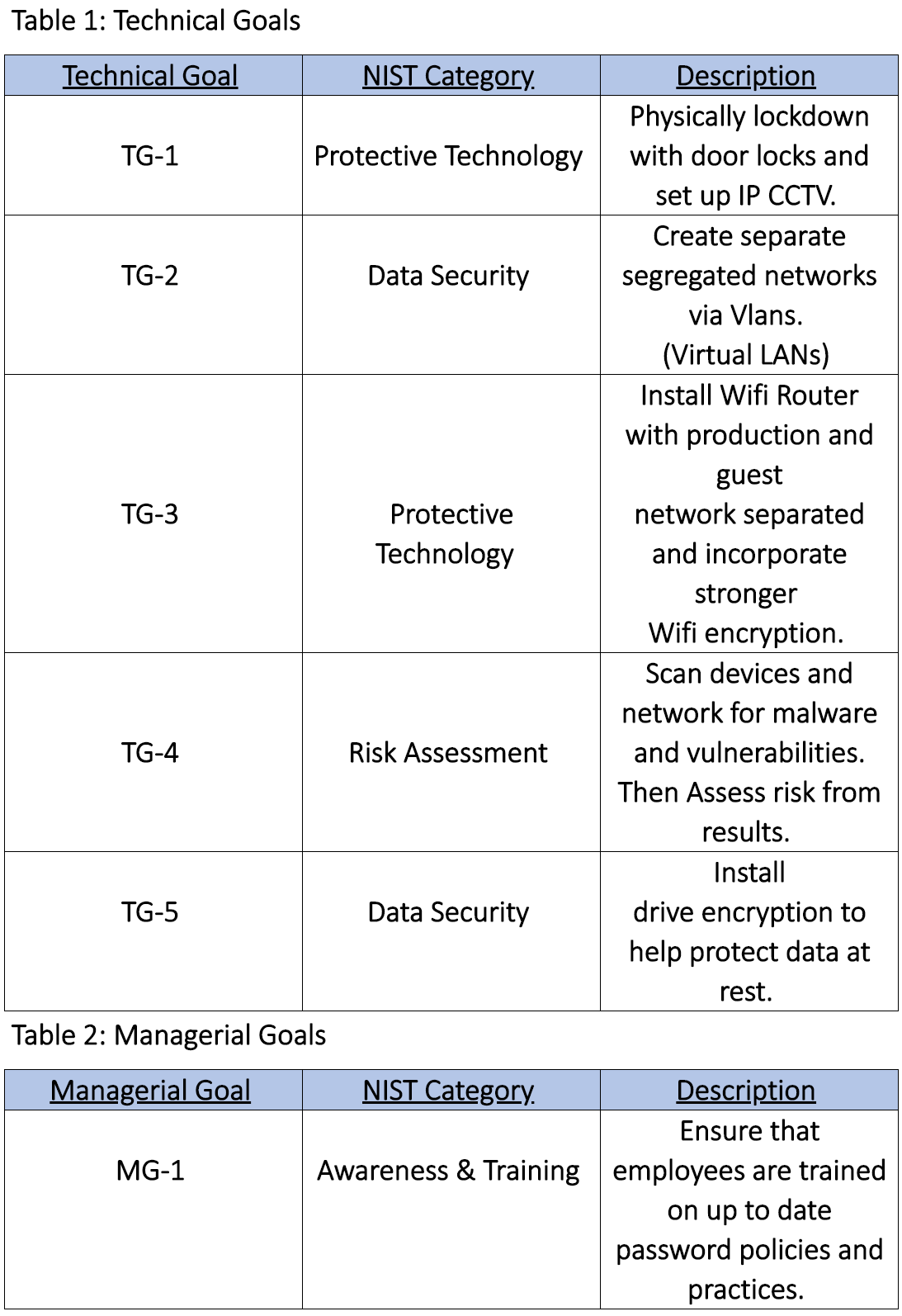
Operation Security issues

* Client only pushes backups to 3rd party but can only use as a restore point, cannot reference live data remotely. Can’t access data in a flash in case of an emergency.

Project Scope and Goals

The goals can be broken into the following categories:

Technical Goals: This involves installing a new Unified Threat Management (UTM) device and physical security controls and is illustrated by Table 1: Technical Goals.

Managerial Goals: These educate employees of top IT security practices to help reduce the risk of security incidents. This is illustrated by Table 2: Managerial Goals.

Recommended Action Plan

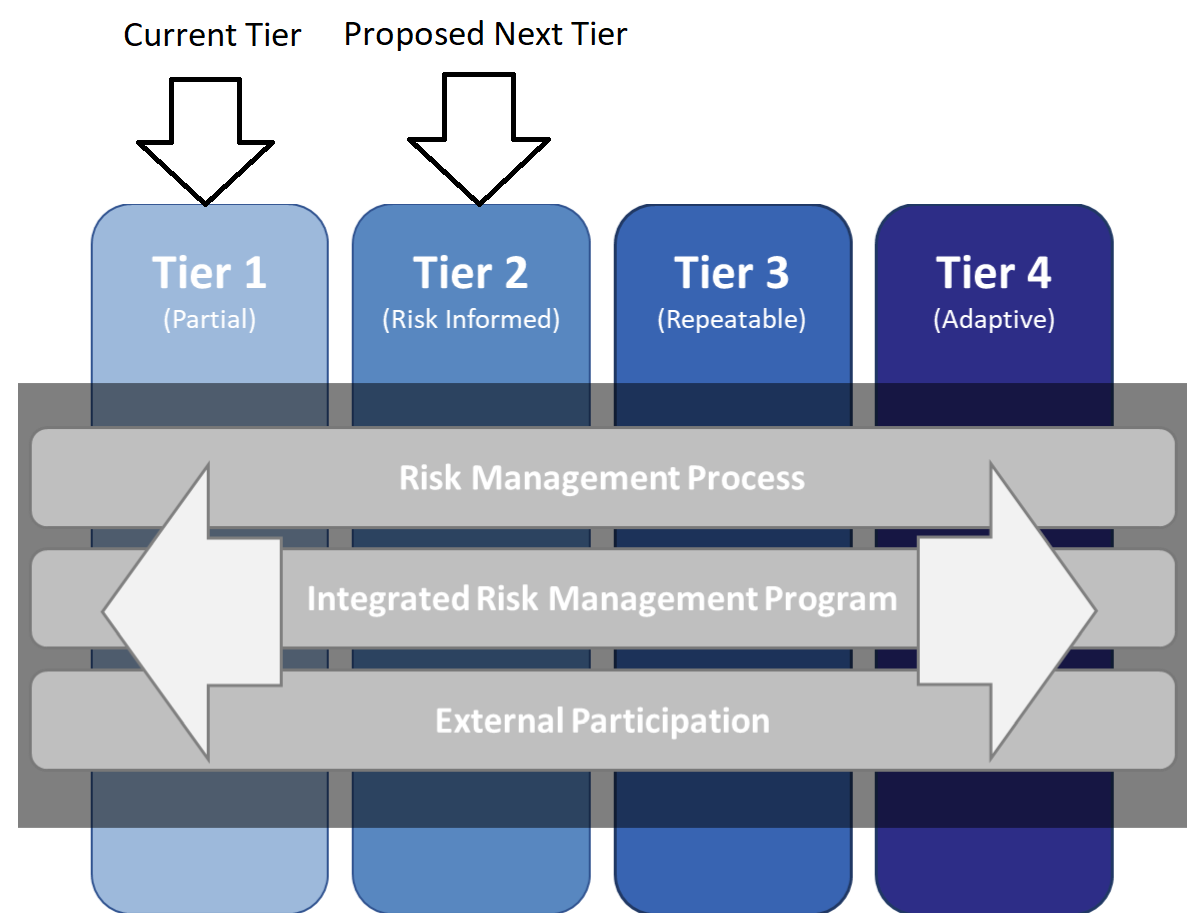
Current NIST Tier Level is: 1

This organization showed limited knowledge about cybersecurity, making it quite accessible and starting it at a NIST Tier 1.

Proposed Target NIST Tier Level is: 2

Within this network security overhaul, this organization will contain management approved processes for deployment of security constructs, will have a somewhat high level of awareness of its own security posture, and have enough digital and physical resources to maintain a loosely coordinated security posture. Raising it from a NIST tier level 1 to a Tier 2.

Image 1: Tier Levels



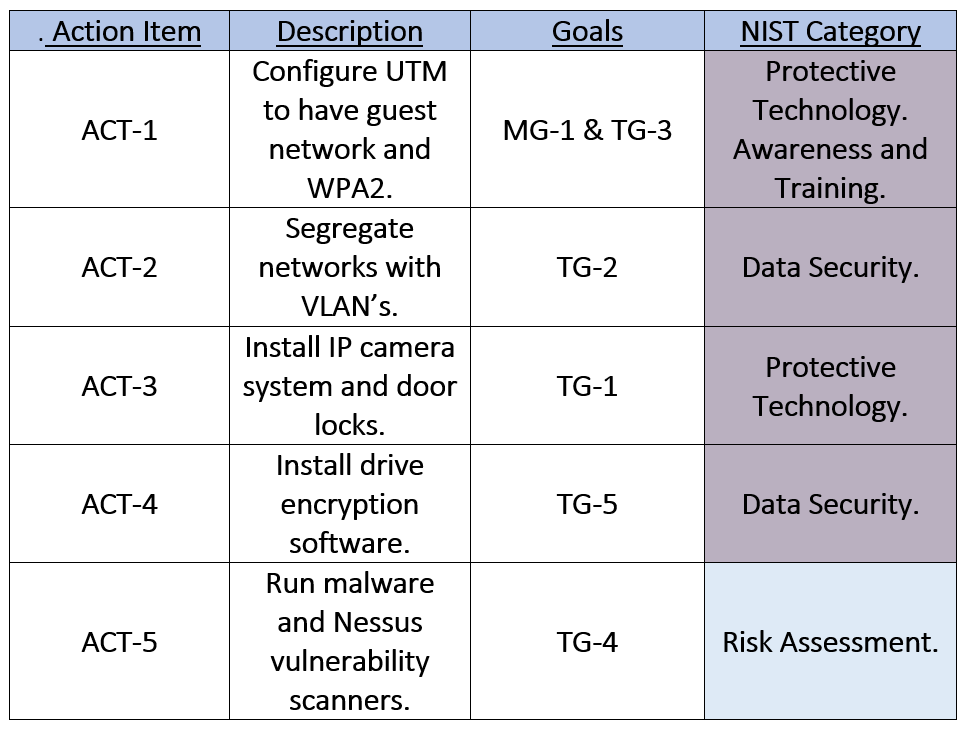


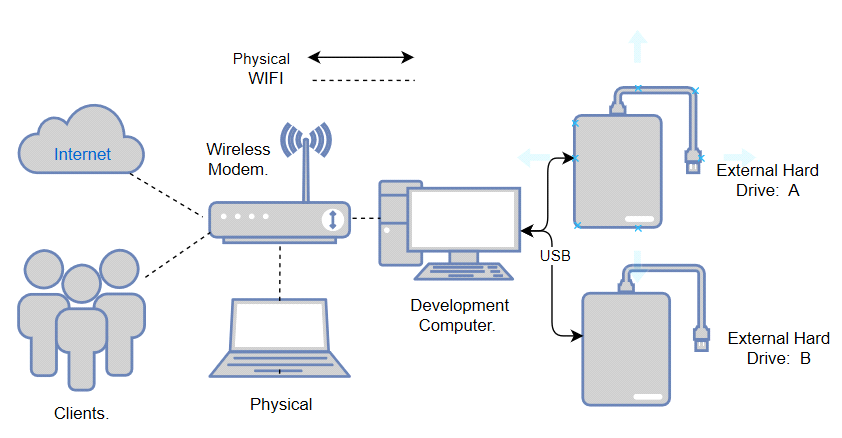
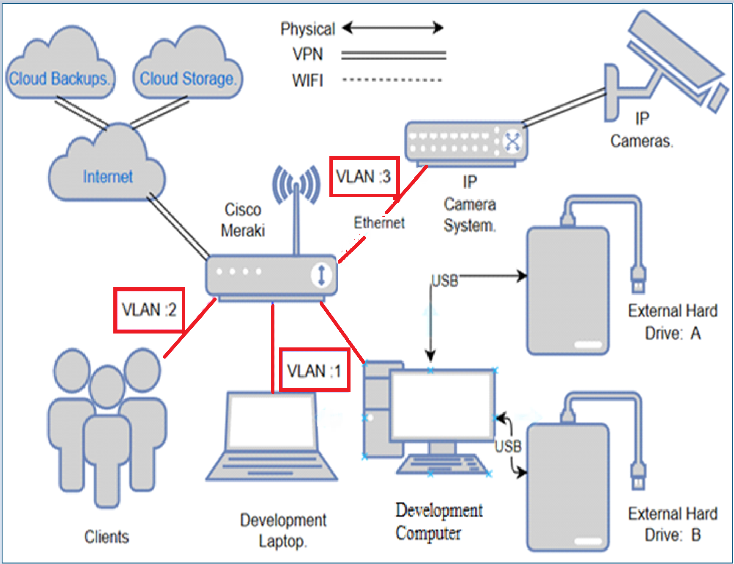
Table 3: Action Plan

Network Topology

This network is originally a flat network by design with no segregation of data in between (See Figure 1). With the new proposed project, the network will incorporate smart switching capabilities along with added confidentiality by a VPN (See Figure 2).

**Figure 2: Proposed Topology After Implementation of the Project**

**Figure 1: Current Topology**



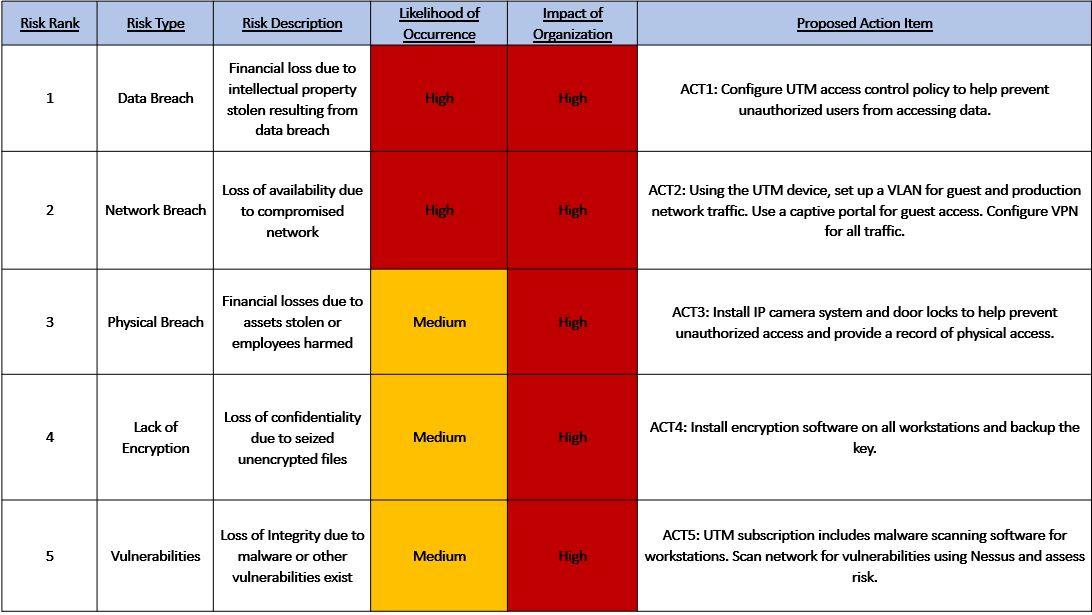
Risk Management Analysis (RMA) Outline

Table 4: Risk Management Analysis

# Anticipated Results

Create segregated networks between production, guest, and IP camera system environments.

* This increases security and mitigates guest accessing the production network or Closed Caption TV (CCTV) network.

Increase Security from WPA to WPA2

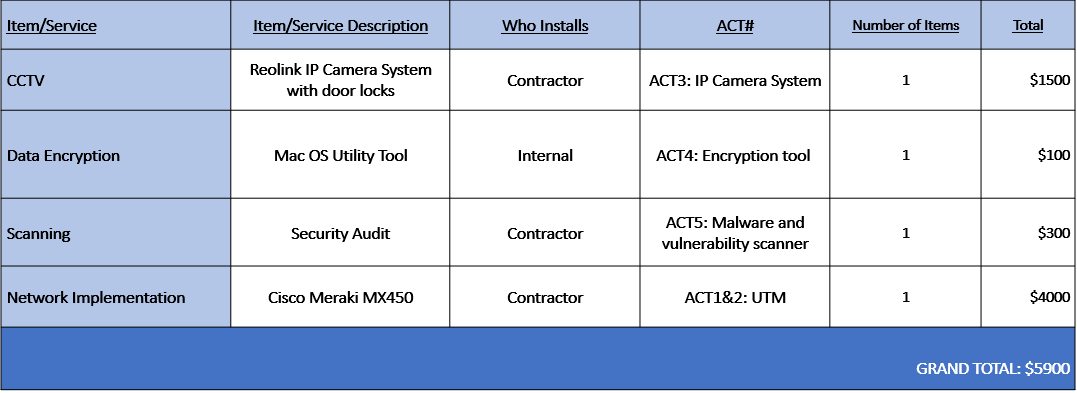
* This increases security because WPA is relatively weak and can be cracked by a brute force attack. WiFi Protected Access 2 (WPA2) increases the WiFi security posture.

Increase Security for Communication to Outside World

* This is done through the VPN and Proxying capabilities of the Meraki network appliance. This reduces the risk of eavesdropping and using the Proxy will mask the packets hops out to the world.

Data Encrypted on Local Machine

* This also reduces the risk of data theft, if a bad actor were able to gain access to the computer. The files are encrypted and will be harder to retrieve without the decryption key.

Proposed Costs

Conclusion

This project focus was to harden the network and raise the cybersecurity posture of an audio engineering facility. Since there was little to no cybersecurity coordination, this audio engineering studio had a NIST Cybersecurity Framework (2014) Tier 1. Physical security can be increased with the installation of door locks and a private Internet Protocol (IP) camera network. Network security can be improved with the introduction of a Network Security Appliance (NSA), in this case being a Meraki all in one device. This will increase security through its abilities to provide a VPN, segregating networks, proxying capabilities, and improving WiFi security from WPA to WPA2. The operation security of this business will be further developed to include disk encryption software to protect data at rest and to also include encrypted connections to a hot cloud drive for more available content management. Once these objectives are completed, this business will then have a stronger cybersecurity posture and higher level of consciousness when it comes to their cyber awareness. It will also provide enough resources to adequately accommodate their cybersecurity needs. After these changes have been made this audio engineering studio will have a new higher proposed NIST Cybersecurity Framework (2014) Tier 2.

Reference

Bhattacharya, D. (2015, September). Evolution of cybersecurity issues in small businesses. *Proceedings of the 4th Annual ACM Conference on Research in Information Technology* (pp. 11- 11).

Jordan, S. (2012). Defense in depth: Employing a layered approach for protecting federal government information systems.

Leyshon, A. (2014). Reformatted: Code, networks, and the transformation of the music industry. Oxford University Press, USA.

Lihong, Y., & Zhiguo, W. (2018, September). Research and design of multi dimension protection system for data security in cloud computing environment. *Proceedings of the 2018 International Conference on Information Hiding and Image Processing* (pp. 12-15).

Ma, S., Lee, K. H., Kim, C. H., Rhee, J., Zhang, X., & Xu, D. (2015, December). Accurate, low cost and instrumentation-free security audit logging for windows. *Proceedings of the 31st Annual Computer Security Applications Conference* (pp. 401-410).

McDermid, D. C., Mahncke, R. J., & Williams, P. A. (2009). Challenges in improving information security practice in Australian general.

Monshizadeh, M., Naldurg, P., & Venkatakrishnan, V. N. (2014, November). Mace: Detecting privilege escalation vulnerabilities in web applications. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 690-701).

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure

cybersecurity Version1.1. US Department of Commerce. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

Xie, R., & Gamble, R. (2013, January). An architecture for cross-cloud auditing. *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop* (pp. 1-4).



Certification of Authorship of Assignment

Submitted to (Professor’s Name): Yair Levy, Ph.D.

Team’s Name/Number: ISEC690-1: Code n Infrastructure

Students’ Names: Babatunde Somade Eric Webb

Date of Assignment: 11/20/2020

Title of Assignment: A Network Hardening and Data Breach Mitigation of an Audio Engineering Studio

Certification of Authorship: By submitting this document we certify that we are the authors of this paper and that any assistance we received in its preparation is fully acknowledged and disclosed in the paper. We have also cited any sources from which we used data, ideas or words, either quoted directly or paraphrased. We also certify that this paper was prepared by us specifically for this course.

Students’ Signatures: Babatunde Somade Eric Webb