Summer, 2020

Security Assessment and Compliance Strategy for a Small Dental Practice

Student: Roy Campbell | Business Advisor: Jack Daniels | Professor: Dr. Yair Levy, Professor of IS & Cybersecurity

Introduction

Healthcare organizations hold, process, and maintain patient information (Gallagher, 2012). These organizations are trusted to maintain the privacy, confidentiality, and integrity of such information (Mohammed, 2015). Cybersecurity in the healthcare sector faces additional challenges due to severe consequences of infrastructure failure or data breaches (Fowler, 2016). While these consequences may not be as catastrophic in the dental industry vertical, the impact of a data breach that leads to exposure of sensitive private information can lead to reputational and legal consequences for a dental practice owner (Takach, 2016). Additionally, collateral identity damage to dental patients such as identity theft and abuse due to exposure of Personally Identifiable Information (PII) can result (Le Bris et al. 2017). The goal of this project will be to develop a security policy and compliance strategy which will protect the privacy and security of the information assets of a small dental practice. This project will gather the data requirements of the practice, analyze the current state of their security profile, assess their needs and seek opportunities for security improvements. Finally, this project will provide a solution comprising a security and compliance plan for the dental practice. The assessment, the solution, and its implementation will be based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework, together with guidelines from the Health Information Portability and Accountability Act (HIPAA). The anticipated results from this project is the progression of Perfect Smile Dental Associates (PSDA) from a Tier 1 to at least Tier 2 level of the NIST Cybersecurity Framework scale.

Problem

Guidelines and regulations such as HIPAA and the privacy act at the federal level, together with various statutes at the state level currently exist to protect the privacy and ensure the security of PII in the health sector (DHS, 2016). However, the protections afforded by these guidelines and regulations are only as effective as the policies, compliance plans and actions of the entities entrusted with healthcare information. In a wide-ranging study of the U.S. healthcare sector, Mohammed et al. (2015) concluded that progress in cybersecurity policy and compliance could only be achieved when reactionary measures are enhanced with a proactive analysis of threat vectors on the horizon. To continue to meet the objectives of safeguarding patient information, maintaining trust in the system of records, and protecting their information assets, the office of the National Coordinator for Health Information Technology recommends best practices for implementation of policies and compliance plans (DHS, 2015).

Facts

This proposed project will focus on a small dental practice, Perfect Smile Dental Associates (PSDA). Organizationally, the dental practice has no dedicated role for cybersecurity. This is usually the norm for a Small or Medium Business (SMB) of this size (Martins, 2019). However, this means that at the company, information security is everyone's problem. Without a dedicated security role, the office manager is the de-facto information security manager. However, the manager is not trained in Information Technology (IT) and has very little awareness of information security. The office manager is aware of HIPAA compliance, but no policy or governance documents are maintained or kept up to date in the practice. Given that about 61% of data breaches directly affect SMBs, together with the fact that about 60% of SMBs fail within six months of a cyberattack (Martins, 2019) then PSDA would be well served by using an external consultant to service its cybersecurity needs. Culturally, there is a high level of trust between the rest of the dental staff and the office manager. While there is a high level of awareness of physical threats to the office, there is a much lower level of awareness of information security threats. However, both the dental staff and the office manager are open to being interviewed about information security and are willing to work towards improving their company cybersecurity profile. Technologically, there are no strong password policies in place or enforced. Sticky notes with passwords stuck to monitors. Additionally, there is no awareness of the impact of links from potentially suspicious emails, no training on recognition of suspicious emails, and an over-reliance on the spam filters of Microsoft Outlook. However, high false positive rate is causing some important emails to sometimes be considered spam. Backups are not automated or consistently done. Dental records are maintained on an on-site server on an internal network. This is complicating expansion plans since it will become complicated to share information between the two dental sites. There are also inefficiencies when transferring records to and from other practices (when new patients bring in records from other practices or PSDA needs to send patient data to other practices or to a hospital). This means that sometimes the fastest way to send the information is through x-ray films that the patient carries over to the other practice). Patient registration is through paper forms that include SSN entry. There is an in-house shredder, but sometimes patients or staff discard partially filled forms in the trashcans.

Project Scope & Goals

Project Scope and Goals: The goal of this project is the development of an Information Security Policy (ISP) development and compliance plan for a small dental practice. The scope of the project will span governance, as well as the identification, protection, and detection of threats in the following areas – based on the highlighted NIST guidelines:

ID.GV-1	HIPAA Compliance
ID.RA-3	Email System
ID.AM-2	Inventory of Installed Software
ID.AC-4	Software Access Permissions and Authorization
PR.IP-6	Retention and Destruction of Data
DE.CM-8	Virus and Vulnerability Scans

Managerial goals will consist of the creation of the ISP and a compliance plan to ensure that identified risks are properly addressed. A set of policies addressing each of the areas in scope will be provided to the management team of PSDA.

Technical goals will consist of application of NIST Cybersecurity Framework guidelines to the compliance processes that will be recommended for addressing the vulnerabilities discovered in email, system and software inventory, data life-cycle management, and virus/malware scans.

Recommended Solution

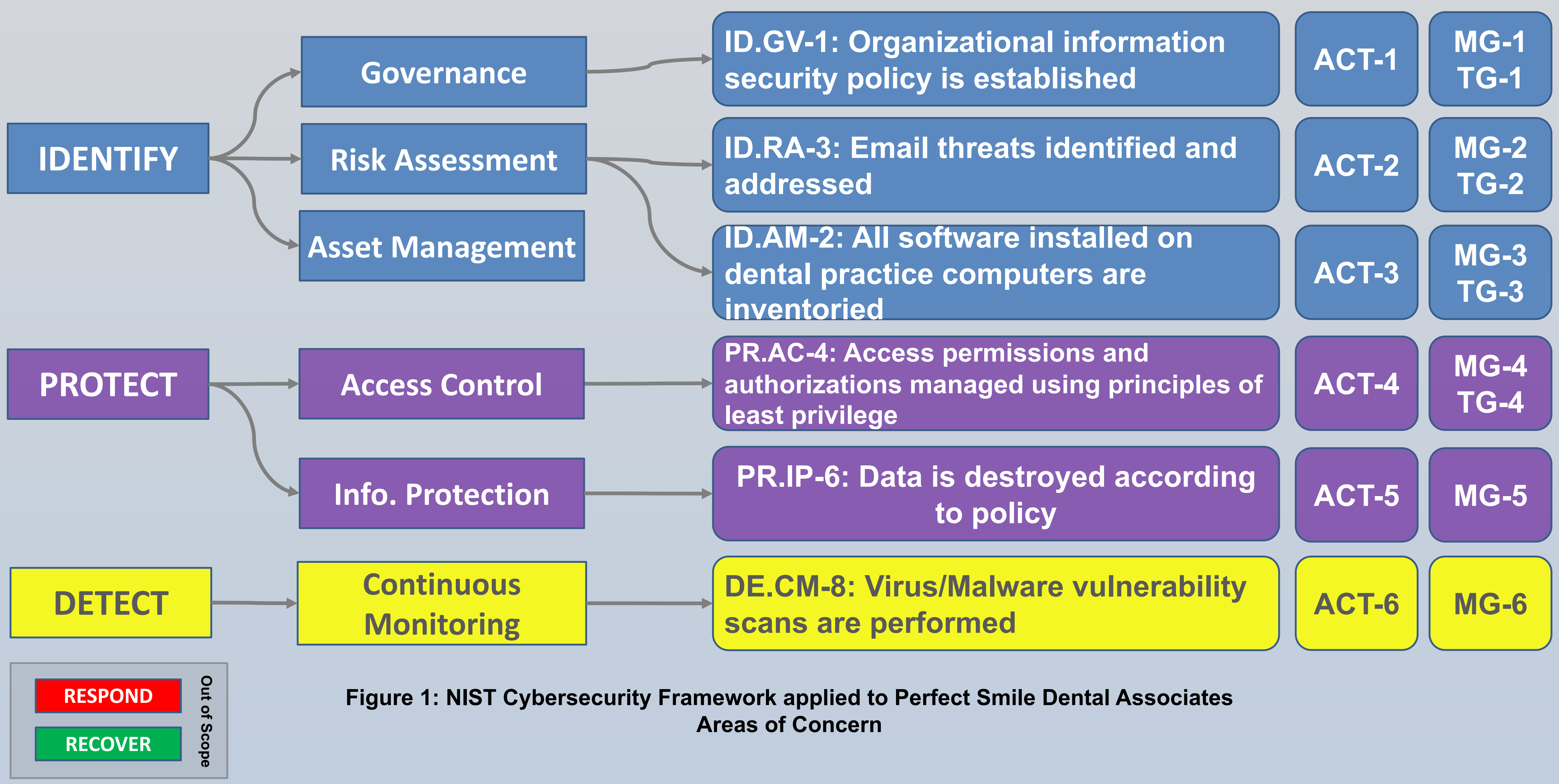

IDENTIFY
Governance
Risk Assessment
Asset Management
ID.GV-1: Organizational information security policy is established
ACT-1
MG-1
TG-1
ID.RA-3: Email threats identified and addressed
ACT-2
MG-2
TG-2
ID.AM-2: All software installed on dental practice computers are inventoried
ACT-3
MG-3
TG-3
PROTECT
Access Control
Info. Protection
PR.AC-4: Access permissions and authorizations managed using principles of least privilege
ACT-4
MG-4
TG-4
PR.IP-6: Data is destroyed according to policy
ACT-5
MG-5
DETECT
Continuous Monitoring
DE.CM-8: Virus/Malware vulnerability scans are performed
ACT-6
MG-6
RESPOND
RECOVER
Out of Scope

Figure 1: NIST Cybersecurity Framework applied to Perfect Smile Dental Associates Areas of Concern

Action Plan

Table 1: Action Plan

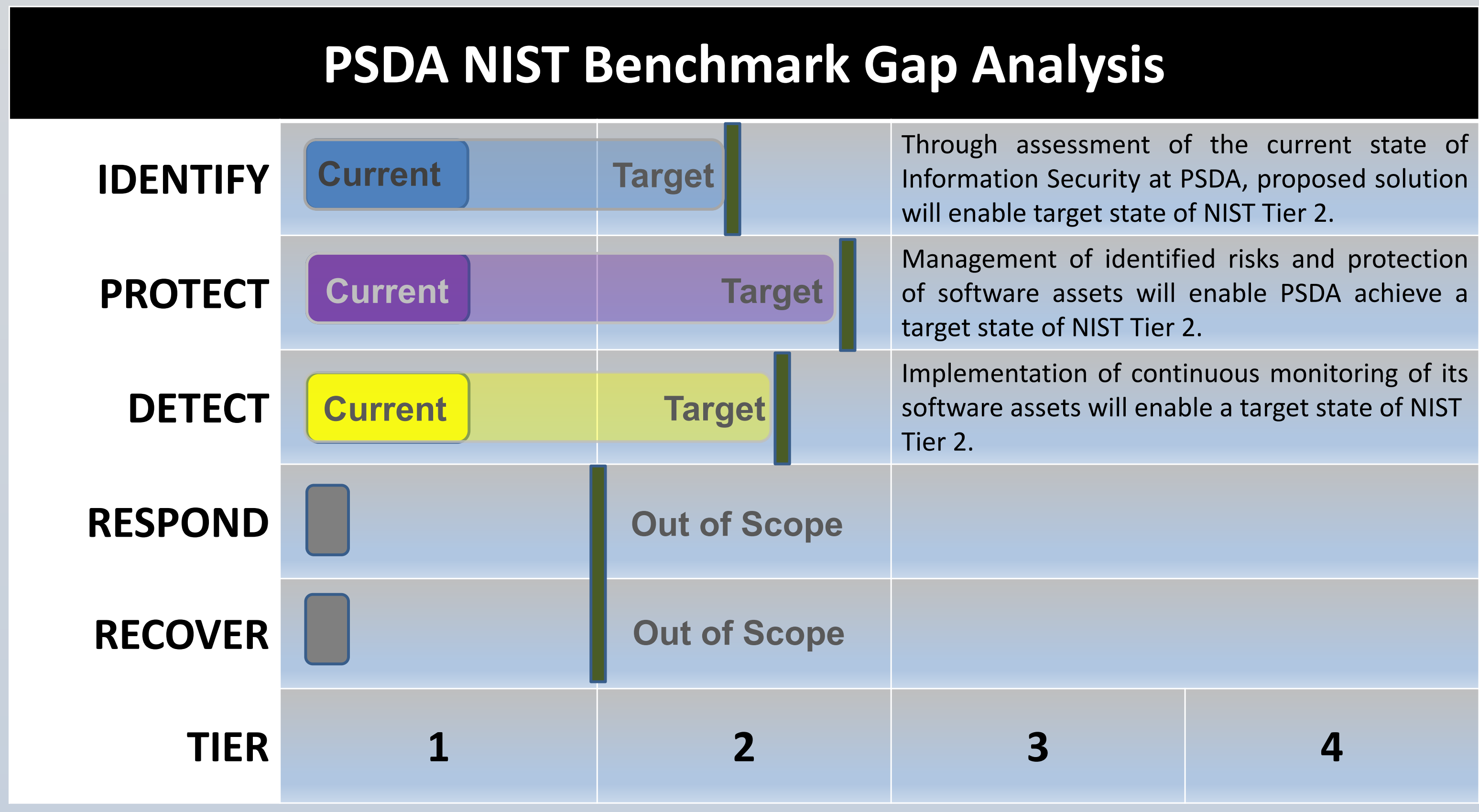
No.	Action Item	Action Description	Type	Goal
ACT-1	Develop and implement an Information Security Plan and a set of compliance policies for the staff and management of Perfect Smile Dental Associates	Education of staff about information security assessment and description of governance policy to assure security compliance for the business	Managerial	MG-1
		Documentation of information security assessment and production of policy documents covering areas of concern identified in Figure 1	Technical	TG-1
ACT-2	Through training, improve awareness of how external threats can materialize through the email system, and configure Microsoft Outlook to reduce the probability of phishing attacks	Train staff on how to recognize suspicious emails	Managerial	MG-2
		Implement whitelisting, spam filters, and relay restrictions	Technical	TG-2
ACT-3	Perform initial vulnerability scan for viruses and malware. Provide automated scheduled vulnerability scanning	Educate staff on importance of regular vulnerability scans	Managerial	MG-3
		Review and fine-tune Windows Defender. Provide additional tools for vulnerability scans and set up real-time virus and malware scanning	Technical	TG-3
ACT-4	Create inventory of all software installed on practice desktops and laptops and establish policy of acceptable software use	Create acceptable use policy for software	Managerial	MG-4
		Document all software (and versions) found, remove software not required for business purposes and enable software installation based on administrative privileges	Technical	TG-4
ACT-5	Set policies and implement controls for access to customer information	Provide guidance on passwords and create policy document access to customer information.	Managerial	MG-5
ACT-6	Set policy for destruction of aged paper records and electronic health records	Review document life-cycle for paper documents and provide policy for secure shredding	Managerial	MG-6

Risk Management Analysis

Table 2: Risk Management Analysis

Rating	Risk	Likelihood	Impact	Mitigation Plan	Action ID
1	Compromised patient records due to lack of HIPAA compliance	High	High	Provide assessment and awareness of areas of information security non-compliance, document and educate management and staff on threats and vulnerabilities which are causing exposure to non-compliance.	ACT-1
2	Financial losses can result from email vulnerabilities	High	High	Provide training on recognition of suspicious emails. Implement whitelisting, spam filters, and relay restrictions.	ACT-2
3	Loss or corruption of data due to viruses or malware	Medium	High	Carry out full vulnerability scan for malware and set up an automated scanning schedule. Properly configure Windows Defender on all company laptops. Educate users about virus and malware threats.	ACT-3
4	Potential data breach due to malware from undocumented and unknown software and processes running on business computers	Medium	High	Carry out full inventory of all software and processes running on company computers in order to identify and remove potentially harmful software and any software not required for business purposes. Create an acceptable use policy for company computers.	ACT-4
5	Patient records can be compromised due to use of a single username and weak password.	Low	High	Educate staff about the importance of strong passwords and set up access policy restricting permissions to customer data to office manager and practice director as required by HIPAA regulations. Put password policy in place to guide future changes to passwords.	ACT-5
6	Legal and financial exposure can result from loss of physical paper patient records held in unlocked cabinets.	Low	Medium	Review paper document life-cycle. Recommend use of cross-cut shredder for paper records no longer required to be held (for example for deceased patients). Recommend electronic scanning and secure storage of paper documents requiring to be maintained.	ACT-6

Anticipated Results



Through assessment of the current state of Information Security at PSDA, proposed solution will enable target state of NIST Tier 2.

Management of identified risks and protection of software assets will enable PSDA achieve a target state of NIST Tier 2.

Implementation of continuous monitoring of its software assets will enable a target state of NIST Tier 2.

Figure 2: Proposed Implementation Tier Change Anticipated for Solution

Proposed Costs

Table 3: Proposed Cost of Solution

Action ID	Service Provided	Personnel	Cost (per hour)	# Items (hours)	Subtotal
ACT-1	Security assessment and Information Security Consultation	Contractor	$125	8	$1,000
ACT-2	Training on email vulnerability awareness. Implementation of spam filtering, whitelisting, and mail relay restrictions.	Contractor	$125	16	$2,000
ACT-3	Malware vulnerability scanning of all business computers.	Contractor	$100	8	$1,000
ACT-4	Create inventory of all software installed on business computers.	Internal	$12	16	$192
ACT-5	Policies and administrative access controls.	Contractor	$125	16	$2,000
ACT-6	Create policy for life-cycle management of paper records.	Contractor	$100	8	$800
			Grand Total	72 hours	$6,992

Conclusion

This project proposal describes the current state of PSDA. It outlines a strategy for elevating the NIST Tier Implementation Level from 1 to 2 through an assessment of the current state of cybersecurity and a plan to address the shortcomings noted during data gathering. It is estimated that about 72 hours of effort from an information security consultant will be required to provide the analysis and implementation of the Information Security solution.

References

Fowler, K. (2016). *Data breach preparation and response: Breaches are certain, impact is not*. \Syngress.

Gallagher, P.D., Blank, R.M. (2012). Guide for conducting risk assessments. *NIST Special Publication 800-30*, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

HIPAA Regulations 164.310 (2020). *Physical safeguards*. http://www.hipaasurvivalguide.com/hipaa-regulations/164-310.php

Le Bris, A., & El Asri, W. (2017). *State of cybersecurity & cyber threats in healthcare organizations.* https://blogs.harvard.edu/cybersecurity/files/2017/01/risks-and-threats-healthcare-strategic report.pdf

Martins, A. (2019). *Cyberattacks and your small business: A primer for cybersecurity.*

Mohammed, D., Mariani, R., & Shereeza, M., (2015). *Cybersecurity challenges and security issues within the U.S. healthcare sector.* https://blogs.harvard.edu/cybersecurity/files/2017/01/risks-and-threats-healthcare-strategic-report.pdf

NIST special publication 800-30. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

NIST cybersecurity framework (2020). https://www.nist.gov/cyberframework

Orthopaedic and Neurosurgery Specialists [ONS] (2020). *Email policy template*. https://onsmd.com/wp-content/uploads/sites/43/2019/01/ONS_email_policy.pdf

Takach, G. S. (2016). Preparing for breach litigation. *Data breach preparation and response.* Syngress.

US Department of Health and Human Services (DHS) (2015). *Guide to privacy and security of electronic health information.* https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

U.S. Department of Health and Human Services (2016). *Security risk analysis tip sheet: Protect patient health information.* https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/2016_SecurityRiskAnalysis.pdf

NOVA SOUTHEASTERN UNIVERSITY | NSU Florida

Center for Information Protection, Education, and Research (CIPhER)
https://InfoSec.nova.edu/

College of Computing and Engineering (CCE)