RISK ASSESSMENT REPORT OF TINES

Cyber Security Measures

PARTICIPANTS

GLADYS MWANGI - Researched and made notes on the report

BLESSING OBASI - Contributed and analysed errors on the report

JANET OLUWATOYIN OLABODE - Contributed and designed the assignment

SUMMARY

The purpose of this risk assessment is to produce a report identifying vulnerabilities and threats related to the consortium of dental practitioners in the Isle of Wight, Tines.

This risk assessment is utilized to identify risk mitigation plans for Tines. The report is made due to the concerns being raised by the staff and patients about the security state of the practices as well as the consortium.

ASSETS ASSOCIATED WITH THE ORGANIZATION

PEOPLE	TECHNOLOGY	PROCESSES
Staff’s Information	PCs	Backup Plans
Patient’s Information	CCTV	Training materials
	Servers	System documentation
	Switches	Organizational policies
	Softwares	Compensating Control Plan

THREATS ASSOCIATED WITH THE ASSETS

- Malwares
- Identity Theft
- Phishing Attacks
- Denial Of Service
- Equipment Theft/ Vandalism
- Insider Threats & Malicious Intent

VULNERABILITIES ASSOCIATED WITH THREATS

- Lack Of Monitoring Controls
- Lack Of Proper Documentation
- Inadequate Technical Support To Staffs
- Lack Of Proper/ Regular Backup System
- Unauthorized Penetration Of The Premise - Physical Break-Ins
- Lack Of Proper Guidelines Or Policies & Training To The Staff Regarding Security Issues

MITIGATION MEASURES FOR THE THREATS

GENERAL MITIGATION MEASURES

- Implementing access control
- Setting up policies and procedures
- Limit duration of access information
- Deploy endpoint security and software
- Limit privileges & Role-based access control
- Use of multifactor authentication and single sign in

INSIDER ATTACKS

- Implement multi-factor authentication in addition to use of password
- Limit staffs' access to only the specific resources needed for their jobs
- Train new employees and contractors on security awareness before access the consortium’s network.
- Incorporate information about unintentional and malicious insider threat awareness into regular security training
- Install employee monitoring software to help reduce the risk of data breaches & theft of intellectual property by identifying careless, disgruntled or malicious insiders

VIRUSES & WORMS

- Keep that software up to date
- Avoid downloading free software from untrusted websites.
- Install antivirus and antimalware software on all their systems and networked devices
- Train users not to download attachments or click on links in emails from unknown senders

DRIVE-BY DOWNLOAD ATTACKS

- Install security software that actively scans websites can help protect endpoints from drive-by downloads
- Regularly update and patch systems with the latest versions of software, applications, browsers, and operating systems

EQUIPMENT THEFT/ VANDALISM

- Hire security guards
- Physical access control
- Develop a security plan
- Proper watch of surveillance cameras

RANSOMWARE

- Users should avoid clicking on links in emails or opening email attachments from unknown sources
- Users should regularly back up their computing devices and update all software, including antivirus software

COMPROMISE OF CONFIDENTIAL INFORMATION

- Limit privileges
- Role based access
- Physical access control
- Implementing access control
- Update and backup of system

IDENTITY THEFT

- Physical access control
- Multi-factor authentication

SOURCES

- Defining Cyber Assets
- Cyber Assets
- Cyber Security Threats
- OWASP TOP 10