Week 6 Assignment - AMC Assessment

805008593
Tim Cockerham
4/1/23
ISTM 635 701
An Aggie does not lie, cheat, or steal or tolerate those who do.

Tier 1 Threats 3
Table 1 - Assets 3
Table 2 - Vulnerabilities 4
Table 3 - Threat Identification 6
Table 4 - Likelihood of Threat 9
Table 5 - Impact of Threat 14
Table 6 - Risk to IT Assets 19
Table 7 - Risk Mitigation 23
Appendix A - Vulnerability Details 26

Tier 1 Threats

According to NIST 800-30 Rev. 1, a tier 1 threat is something that increases the possibility of “damage to image or reputation of the organization or financial loss” (Joint Task Force Transformation Initiative). Aggieland Medical Center (AMC) has several threats but two tier 1 threats are being hacked and natural disasters.

If AMC got breached by hackers who stole sensitive patient information, customers would need to follow the increasingly normal process of monitoring their credit, changing passwords, etc. However, if it was later proven that the breach occurred due to negligence on the part of AMC, it could be catastrophic to the business. Customers may never return to a business that was irresponsible with their data.

AMC has a large history of patient data in paper format in the building. If the area were to experience a disaster like a tornado, flood, or fire, they would likely lose all of that customer data. As with the breach discussed above, customers may never return to a business that kept all of their data in a volatile format like paper.

Table 1 - Assets

A list of Aggieland Medical Center’s IT assets, grouped by operating system.

Categories	**Operating System**	**Asset(s)**
Workstations	Windows 7	PCs - Administrative offices, emergency rooms
	Windows 10	PCs - Treatment rooms, physicians’ offices
	Red Hat Linux 6	Labs
Servers	Windows Server	Patient Data Information Server (PDIS), Financial Record Keeping Server (FRKS), Personnel Management Server (PMS), Medical Logistics Server (MLS), Emergency Care Data System (ECDS), Pharmacy System (RxS)
Server	Red Hat Linux 6	Email
Firewall	Cisco ASA	Firewall server used to

		manage the organization's firewall
Router	Cisco 2951	Router used to connect the organization's network
Switches	Cisco SG100D-08-NA	Switches used to connect workstations and servers

Table 2 - Vulnerabilities

This table is a list of the vulnerabilities associated with the assets in table 1.

Asset ID	**Description**	**Vulnerability**	**Evidence**
W7	Workstations running Windows 7	CVE-2015-6131	Pen testing report
		CVE-2015-6127	Pen testing report
		One staff stays logged into workstations for multiple users	Page 13
		Users share passwords	Page 13
		Customers can read info on screens	Page 13
		Doctors and nurses discuss patient info in open areas	Page 13
		Staff view unauthorized patient records	Page 14
W10	Workstations running Windows 10	CVE-2022-21851	Pen testing report
		CVE-2022-21922	Pen testing report
		Auto logout after inactivity is inconsistent in patient rooms	Page 14, table 9, Staff Areas of Concern
RH6	Workstations and servers running Red	CVE-2000-0633	Pen testing report
		CVE-2000-0219	Pen testing report

	Hat Linux 6		
MSSQL	Servers running Sql Server	CVE-2022-29143	Pen testing report
		CVE-2021-1636	Pen testing report
		PDIS can be accessed directly from outside firewall	Page 8, Table 2
		Users have more access in PDIS than needed	Page 11, Table 5
		Users enter wrong data in systems, resulting in wrong records and/or duplicate records	Page 11, Table 5
		No one trained to read vulnerability assessment reports	Page 14
		Delayed response to breach report	Page 14
		Unfamiliarity with disclosure regulations results in confidential info released to insurance or press	Page 15
		Email system used to discuss treatment plans	Page 15, Table 9
		Email system appointments can be seen by external entities	Page 15, Table 9
		LAN instability causes users to use home computers to transmit patient info	Page 15, Table 9
		Inadequate IT training, inappropriate users trained as IT workers	Page 15, Table 9

Firewall	Server running the Cisco ASA firewall	Not configured correctly leaving systems vulnerable to malware, viruses, and loss of connectivity	Page 11, Table 5
Router	Cisco 2951 Routers	No vulnerabilities	
Switch	Cisco SG100D-08-NA Switches	No vulnerabilities	

Table 3 - Threat Identification

For each of the vulnerabilities in table 2, this table explains what the threat from that vulnerability is and who is likely to exploit it.

Asset ID	**Vulnerability**	**Threat**	**Threat Source**	**Exploit**
W7	CVE-2015-6131	Remote code execution	Outside hackers	Crafted .mcl file (Source: https://nvd.nist.gov/vuln/detail/CVE-2015-6131)
	CVE-2015-6127	Read arbitrary files	Outside hackers	Crafted .mcl file (Source: https://nvd.nist.gov/vuln/detail/CVE-2015-6127)
	One staff stays logged into workstations for multiple users	Inability to audit employee actions. Employees can view unauthorized info	Employees	Employees logged in as another user can view that user's information. Can view info they're not authorized to view.
	Users share passwords	Users can log into workstations as other users	Employees	Employees logged in as another user can view that user's information. Can view info they're not authorized to view.
	Customers can read info on screens	Customers can view info for other customers	Internal customers	Customers can read workstation screens from open areas.

	Doctors and nurses discuss patient info in open areas	Customers can learn info about other customers	Internal customers	Customers can listen to medical personnel discuss other customers' information.
	Staff view unauthorized patient records	Staff view info of patients they personally know	Employees	Employees can log into PDIS and view any patient's records.
W10	CVE-2022-21851	Remote code execution	Outside hackers	See appendix A
	CVE-2022-21922	Remote code execution	Outside hackers	Low privilege user can execute code through the RPC runtime
	Auto logout after inactivity is inconsistent in patient rooms	Read patient data on the screen	Other patients	Read the data from a previous patient on the screen
WRH6	CVE-2000-0633	System reboot or halt	Local users	Allows local users to reboot or halt the system (Source: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0633)
	CVE-2000-0219	Root access	Local users	Boot a single user and hitting ^C at the password prompt (Source: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0219)
MSSQL	CVE-2022-29143	Remote code execution	Outside hackers	Execute a specially crafted query using $ partition against a table with a Column Store index (Source: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-29143)
	CVE-2021-1636	Elevation of privilege	Authenticated hacker	Send data over a network to an affected SQL Server when configured to run an Extended Event session

				(Source: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-1636)
	PDIS can be accessed directly from outside firewall	Database server with patient info can be seen by the internet.	Outside hackers	Hackers can get to a DB server from anywhere, only needing to log into it.
	Users have more access in PDIS than needed	Roles have too many permissions	Employees	Employees can access information that they don't need access to.
	Users enter wrong data in systems, resulting in wrong records and/or duplicate records	End users type in the wrong data giving patients incorrect info or duplicate records	Employees	Employees don't pay attention and type in wrong data.
	No one trained to read vulnerability assessment reports	IT staff get vulnerability reports but don't know what to do with the info, leaving problems unattended	Employees	IT staff get a report of vulnerabilities but don't do anything with the info on it.
	Delayed response to breach report	A "few days" after a breach report gives hackers more time to steal data or destroy systems	External employees	ABC Systems employees are notified about a breach but don't get to AMC for a few days.
	Unfamiliarity with disclosure regulations results in confidential info released to insurance or press	Confidential patient info is released to insurance companies and the press	Employees	Employees aren't trained adequately to know which data is confidential and which can be released safely.
	Email system used to discuss treatment plans	Unsecured email system can be accessed by	Employees	Medical personnel use the unsecured email system to discuss

		more than just medical personnel and their patient		confidential info with a patient.
	Email system appointments can be seen by external entities	Insurance personnel can use appointment records to see private data about patients	External employees	Insurance company personnel can view appointment records to see which of their customers regularly visits the doctor.
	LAN instability causes users to use home computers to transmit patient info	Users use their unsecured and unpatched home computers to handle work duties	Employees	Network instability causes users to use their home computers, regardless of its security level.
	Inadequate IT training, inappropriate users trained as IT workers	Untrained personnel are expected to handle IT problems	Employees	IT staff and medical admins aren't trained enough but are still expected to handle the IT problems.
Firewall	Not configured correctly leaving systems vulnerable to malware, viruses, and loss of connectivity	Firewall leaves internal systems open to attack by viruses, malware, and hackers	External employees	ABC Systems improperly set up the firewall so that it's vulnerable to attack.

Table 4 - Likelihood of Threat

The measurement (definitely, likely, or unlikely) of the possibility the vulnerability will be exploited by a hacker.

Definitely	**Likely**	**Unlikely**
The threat will happen	The threat may happen	The threat won't happen

Asset ID	**Vulnerability**	**Threat**	**Threat Source**	**Exploit**	**Likelihood**

W7	CVE-2015-6131	Remote code execution	Outside hackers	Crafted .mcl file (Source: https://nvd.nist.gov/vuln/detail/CVE-2015-6131)	Definitely
	CVE-2015-6127	Read arbitrary files	Outside hackers	Crafted .mcl file (Source: https://nvd.nist.gov/vuln/detail/CVE-2015-6127)	Definitely
	One staff stays logged into workstations for multiple users	Inability to audit employee actions. Employees can view unauthorized info	Employees	Employees logged in as another user can view that user's information. Can view info they're not authorized to view.	Definitely
	Users share passwords	Users can log into workstations as other users	Employees	Employees logged in as another user can view that user's information. Can view info they're not authorized to view.	Definitely
	Customers can read info on screens	Customers can view info for other customers	Internal customers	Customers can read workstation screens from open areas.	Definitely
	Doctors and nurses discuss patient info in open areas	Customers can learn info about other customers	Internal customers	Customers can listen to medical personnel discuss other customers' information.	Likely
	Staff view unauthorized patient records	Staff view info of patients they personally know	Employees	Employees can log into PDIS and view any patient's records.	Likely
W10	CVE-2022-21851	Remote code execution	Outside hackers	See appendix A	Definitely

	CVE-2022-21922	Remote code execution	Outside hackers	Low privilege user can execute code through the RPC runtime	Definitely
	Auto logout after inactivity is inconsistent in patient rooms	Read patient data on the screen	Other patients	Read the data from a previous patient on the screen	Likely
WRH6	CVE-2000-0633	System reboot or halt	Local users	Allows local users to reboot or halt the system (Source: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0633)	Likely
	CVE-2000-0219	Root access	Local users	Boot a single user and hitting ^C at the password prompt (Source: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0219)	Likely
MSSQL	CVE-2022-29143	Remote code execution	Outside hackers	Execute a specially crafted query using $ partition against a table with a Column Store index (Source: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-29143)	Unlikely
	CVE-2021-1636	Elevation of privilege	Authenticated hacker	Send data over a network to an affected SQL Server when configured to run an Extended Event session (Source: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-1636)	Unlikely
	PDIS can be accessed directly	Database server with	Outside hackers	Hackers can get to a DB server from	Likely

	from outside firewall	patient info can be seen by the internet.		anywhere, only needing to log into it.	
	Users have more access in PDIS than needed	Roles have too many permissions, allowing employees access to information they shouldn't see	Employees	Employees can access information that they don't need access to.	Likely
	Users enter wrong data in systems, resulting in wrong records and/or duplicate records	End users type in the wrong data giving patients incorrect info or duplicate records	Employees	Employees don't pay attention and type in wrong data.	Definitely
	No one trained to read vulnerability assessment reports	IT staff get vulnerability reports but don't know what to do with the info, leaving problems unattended and missing important notices	Employees	IT staff get a report of vulnerabilities but don't do anything with the info on it.	Definitely
	Delayed response to breach report	A "few days" after a breach report gives hackers more time to steal data or destroy systems	External employees	ABC Systems employees are notified about a breach but don't get to AMC for a few days.	Likely

	Unfamiliarity with disclosure regulations results in confidential info released to insurance or press	Confidential patient info is released to insurance companies and the press	Employees	Employees aren't trained adequately to know which data is confidential and which can be released safely.	Likely
	Email system used to discuss treatment plans	Unsecured email system can be accessed by more than just medical personnel and their patient	Employees	Medical personnel use the unsecured email system to discuss confidential info with a patient.	Likely
	Email system appointments can be seen by external entities	Insurance personnel can use appointment records to see private data about patients	External employees	Insurance company personnel can view appointment records to see which of their customers regularly visits the doctor.	Likely
	LAN instability causes users to use home computers to transmit patient info	Users use their unsecured and unpatched home computers to handle work duties	Employees	Network instability causes users to use their home computers, regardless of its security level.	Definitely
	Inadequate IT training, inappropriate users trained as IT workers	Untrained personnel are expected to handle IT problems, causing them to be mishandled	Employees	IT staff and medical admins aren't trained enough but are still expected to handle the IT problems.	Definitely

Firewall	Not configured correctly leaving systems vulnerable to malware, viruses, and loss of connectivity	Firewall leaves internal systems open to attack by viruses, malware, and hackers	External employees	ABC Systems improperly set up the firewall so that it's vulnerable to attack.	Definitely

Table 5 - Impact of Threat

This table shows the measurement of the impact of an attack of each asset listed in Table 1 across the dimensions of confidentiality (how sensitive is the data), integrity (how damaged is the data), and availability (how vital is the data if it were missing).

Critical	Moderate	No Impact
Confidentiality, Integrity, and/or Availability of the target asset are completely compromised	Confidentiality, Integrity, and/or Availability of the target asset are partially compromised	Confidentiality, Integrity, and/or Availability of the target asset are not compromised

Asset ID	Vulnerability	Threat	Threat Source	Exploit	Impact
W7	CVE-2015-6131	Remote code execution	Outside hackers	Crafted .mcl file (Source: https://nvd.nist.gov/vuln/detail/CVE-2015-6131)	Critical
	CVE-2015-6127	Read arbitrary files	Outside hackers	Crafted .mcl file (Source: https://nvd.nist.gov/vuln/detail/CVE-2015-6127)	Moderate
	One staff stays logged into workstations for multiple users	Inability to audit employee actions. Employees can view unauthorized info	Employees	Employees logged in as another user can view that user's information. Can view info they're not authorized to view.	Moderate
	Users share passwords	Users can log into	Employees	Employees logged in as another user can view	Moderate

		workstations as other users		that user's information. Can view info they're not authorized to view.	
	Customers can read info on screens	Customers can view info for other customers	Internal customers	Customers can read workstation screens from open areas.	Moderate
	Doctors and nurses discuss patient info in open areas	Customers can learn info about other customers	Internal customers	Customers can listen to medical personnel discuss other customers' information.	Moderate
	Staff view unauthorized patient records	Staff view info of patients they personally know	Employees	Employees can log into PDIS and view any patient's records.	Moderate
W10	CVE-2022-21851	Remote code execution	Outside hackers	See appendix A	Critical
	CVE-2022-21922	Remote code execution	Outside hackers	Low privilege user can execute code through the RPC runtime	Critical
	Auto logout after inactivity is inconsistent in patient rooms	Read patient data on the screen	Other patients	Read the data from a previous patient on the screen	Moderate
WRH6	CVE-2000-0633	System reboot or halt	Local users	Allows local users to reboot or halt the system (Source: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0633)	No impact
	CVE-2000-0219	Root access	Local users	Boot a single user and hitting ^C at the password prompt (Source: https://cve.mitre.org/cgi-	Critical

				bin/cvename.cgi?name=CVE-2000-0219)	
MSSQL	CVE-2022-29143	Remote code execution	Outside hackers	Execute a specially crafted query using $ partition against a table with a Column Store index (Source: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-29143)	Moderate
	CVE-2021-1636	Elevation of privilege	Authenticated hacker	Send data over a network to an affected SQL Server when configured to run an Extended Event session (Source: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-1636)	Moderate
	PDIS can be accessed directly from outside firewall	Database server with patient info can be seen by the internet.	Outside hackers	Hackers can get to a DB server from anywhere, only needing to log into it.	Critical
	Users have more access in PDIS than needed	Roles have too many permissions, allowing employees access to information they shouldn't see	Employees	Employees can access information that they don't need access to.	Moderate
	Users enter wrong data in systems,	End users type in the wrong	Employees	Employees don't pay attention and type in wrong data.	Moderate

	resulting in wrong records and/or duplicate records	data giving patients incorrect info or duplicate records			
	No one trained to read vulnerability assessment reports	IT staff get vulnerability reports but don't know what to do with the info, leaving problems unattended and missing important notices	Employees	IT staff get a report of vulnerabilities but don't do anything with the info on it.	Moderate
	Delayed response to breach report	A "few days" after a breach report gives hackers more time to steal data or destroy systems	External employees	ABC Systems employees are notified about a breach but don't get to AMC for a few days.	Critical
	Unfamiliarity with disclosure regulations results in confidential info released to insurance or press	Confidential patient info is released to insurance companies and the press	Employees	Employees aren't trained adequately to know which data is confidential and which can be released safely.	Moderate
	Email system used to discuss treatment plans	Unsecured email system	Employees	Medical personnel use the unsecured email system to discuss	Moderate

		can be accessed by more than just medical personnel and their patient		confidential info with a patient.	
	Email system appointments can be seen by external entities	Insurance personnel can use appointment records to see private data about patients	External employees	Insurance company personnel can view appointment records to see which of their customers regularly visits the doctor.	Moderate
	LAN instability causes users to use home computers to transmit patient info	Users use their unsecured and unpatched home computers to handle work duties	Employees	Network instability causes users to use their home computers, regardless of its security level.	Moderate
	Inadequate IT training, inappropriate users trained as IT workers	Untrained personnel are expected to handle IT problems, causing them to be mishandled	Employees	IT staff and medical admins aren't trained enough but are still expected to handle the IT problems.	Moderate
Firewall	Not configured correctly leaving systems vulnerable to malware, viruses,	Firewall leaves internal systems open to attack by	External employees	ABC Systems improperly set up the firewall so that it's vulnerable to attack.	Critical

	and loss of connectivity	viruses, malware, and hackers			

Table 6 - Risk to IT Assets

This table shows the computed risk for each group of IT assets from Table 1.

RISK MATRIX				
	IMPACT			
LIKELIHOOD		**Critical**	**Moderate**	**No Impact**
	Definitely	High	Medium-high	Low
	Likely	Medium-high	Medium	Low
	Unlikely	Low	Low	Low

RISK ESTIMATES						
Asset ID	**Vulnerability**	**Threat**	**Threat Source**	**Likelihood**	**Impact**	**Risk**
W7	CVE-2015-6131	Remote code execution	Outside hackers	Definitely	Critical	High
	CVE-2015-6127	Read arbitrary files	Outside hackers	Definitely	Moderate	Medium-high
	One staff stays logged into workstations for multiple users	Inability to audit employee actions. Employees can view unauthorized info	Employees	Definitely	Moderate	Medium-high
	Users share passwords	Users can log into workstations as other	Employees	Definitely	Moderate	Medium-high

		users				
	Customers can read info on screens	Customers can view info for other customers	Internal customers	Definitely	Moderate	Medium-high
	Doctors and nurses discuss patient info in open areas	Customers can learn info about other customers	Internal customers	Likely	Moderate	Medium
	Staff view unauthorized patient records	Staff view info of patients they personally know	Employees	Likely	Moderate	Medium
W10	CVE-2022-21851	Remote code execution	Outside hackers	Definitely	Critical	High
	CVE-2022-21922	Remote code execution	Outside hackers	Definitely	Critical	High
	Auto logout after inactivity is inconsistent in patient rooms	Read patient data on the screen	Other patients	Likely	Moderate	Medium
WRH6	CVE-2000-0633	System reboot or halt	Local users	Likely	No impact	Low
	CVE-2000-0219	Root access	Local users	Likely	Critical	Medium-high
MSSQL	CVE-2022-29143	Remote code execution	Outside hackers	Unlikely	Moderate	Low
	CVE-2021-1636	Elevation of privilege	Authenticated hacker	Unlikely	Moderate	Low

	PDIS can be accessed directly from outside firewall	Database server with patient info can be seen by the internet.	Outside hackers	Likely	Critical	Medium-high
	Users have more access in PDIS than needed	Roles have too many permissions, allowing employees access to information they shouldn't see	Employees	Likely	Moderate	Medium
	Users enter wrong data in systems, resulting in wrong records and/or duplicate records	End users type in the wrong data giving patients incorrect info or duplicate records	Employees	Definitely	Moderate	Medium-high
	No one trained to read vulnerability assessment reports	IT staff get vulnerability reports but don't know what to do with the info, leaving problems unattended and missing important notices	Employees	Definitely	Moderate	Medium-high
	Delayed response to breach report	A "few days" after a breach report gives	External employees	Likely	Critical	Medium-high

		hackers more time to steal data or destroy systems				
	Unfamiliarity with disclosure regulations results in confidential info released to insurance or press	Confidential patient info is released to insurance companies and the press	Employees	Likely	Moderate	Medium
	Email system used to discuss treatment plans	Unsecured email system can be accessed by more than just medical personnel and their patient	Employees	Likely	Moderate	Medium
	Email system appointments can be seen by external entities	Insurance personnel can use appointment records to see private data about patients	External employees	Likely	Moderate	Medium
	LAN instability causes users to use home computers to transmit patient info	Users use their unsecured and unpatched home computers to handle work duties	Employees	Definitely	Moderate	Medium-high

	Inadequate IT training, inappropriate users trained as IT workers	Untrained personnel are expected to handle IT problems, causing them to be mishandled	Employees	Definitely	Moderate	Medium-high
Firewall	Not configured correctly leaving systems vulnerable to malware, viruses, and loss of connectivity	Firewall leaves internal systems open to attack by viruses, malware, and hackers	External employees	Definitely	Critical	High

Table 7 - Risk Mitigation

This table supplies a mitigation strategy for each threat in table 3.

Asset ID	**Vulnerability**	**Threat**	**Mitigation**
W7	CVE-2015-6131	Remote code execution	Patch systems
	CVE-2015-6127	Read arbitrary files	Patch systems
	One staff stays logged into workstations for multiple users	Inability to audit employee actions. Employees can view unauthorized info	Train employees on the dangers of the behavior and explain disciplinary consequences.
	Users share passwords	Users can log into workstations as other users	Train employees on the dangers of the behavior and explain disciplinary consequences.
	Customers can read info on screens	Customers can view info for other customers	Reconfigure office desks so that screens

			can't be seen by customers.
	Doctors and nurses discuss patient info in open areas	Customers can learn info about other customers	Train employees on the dangers of the behavior and explain disciplinary consequences.
	Staff view unauthorized patient records	Staff view info of patients they personally know	Train employees on the dangers of the behavior and explain disciplinary consequences.
W10	CVE-2022-21851	Remote code execution	Patch systems.
	CVE-2022-21922	Remote code execution	Patch systems.
	Auto logout after inactivity is inconsistent in patient rooms	Read patient data on the screen	Configure all systems to log out after 5 minutes of inactivity.
WRH6	CVE-2000-0633	System reboot or halt	Patch systems.
	CVE-2000-0219	Root access	Patch systems.
MSSQL	CVE-2022-29143	Remote code execution	Patch systems.
	CVE-2021-1636	Elevation of privilege	Patch systems.
	PDIS can be accessed directly from outside firewall	Database server with patient info can be seen by the internet.	Reconfigure firewall to close ports to server.
	Users have more access in PDIS than needed	Roles have too many permissions	Review all role permissions. Configure roles with an appropriate set of permissions.
	Users enter wrong data in systems, resulting in wrong records and/or duplicate records	End users type in the wrong data giving patients incorrect info or duplicate records	Train employees on the need for accurate data entry. Configure data entry system to only allow appropriate data.
	No one trained to read vulnerability assessment reports	IT staff get vulnerability reports but don't know what to do with the info, leaving	Discontinue contract with ABC Systems. Hire more IT staff.

		problems unattended	Retrain all existing staff on the existing systems.
	Delayed response to breach report	A “few days” after a breach report gives hackers more time to steal data or destroy systems	Discontinue contract with ABC Systems. Hire more IT staff. Retrain all existing staff on the existing systems.
	Unfamiliarity with disclosure regulations results in confidential info released to insurance or press	Confidential patient info is released to insurance companies and the press	Train employees on the dangers of the behavior and explain disciplinary consequences.
	Email system used to discuss treatment plans	Unsecured email system can be accessed by more than just medical personnel and their patient	Train employees on the dangers of the behavior and explain disciplinary consequences.
	Email system appointments can be seen by external entities	Insurance personnel can use appointment records to see private data about patients	Reconfigure email system to only allow AMC employee access.
	LAN instability causes users to use home computers to transmit patient info	Users use their unsecured and unpatched home computers to handle work duties	Repair LAN and train employees not to use home computers for work.
	Inadequate IT training, inappropriate users trained as IT workers	Untrained personnel are expected to handle IT problems	Discontinue contract with ABC Systems. Hire more IT staff. Retrain all existing staff on the existing systems.
Firewall	Not configured correctly leaving systems vulnerable to malware, viruses, and loss of connectivity	Firewall leaves internal systems open to attack by viruses, malware, and hackers	Reconfigure firewall using best practices.

Appendix A - Vulnerability Details

Vulnerability	Threat	Threat Source	Exploit
CVE-2022-21851	Remote code execution	Outside hackers	An authenticated user could be tricked into connecting to a malicious remote desktop server where the remote desktop host server sends a specially crafted PDU (Server RDP Preconnection) that targets the remote client's drive redirection virtual channel. The end result could lead to remote code execution on the victim's machine. (Source: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-21851)

Work Cited

Joint Task Force Transformation Initiative. “NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments.” *NIST Technical Series Publications*, September 2012, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf. Accessed 1 April 2023.