Assignment 1

In Part 2, you will be presented with six sections of a scenario. Each section is accompanied by questions. You must navigate back to the Instructions page to access the sections. Please answer all questions for all sections in the same document. Submit the completed document after you have worked through all six sections.

Section 1

A. Navigate to the Instructions page to access Section 1 Scenario.

B. Answer the following questions:

1. Is this considered a HIPAA breach? If unable to determine this yet, what additional information is needed to determine this? HIPAA reference: <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>

2. Who needs to be notified regarding the incident at this point [Incident Response (IR) team, EMR vendor, law enforcement, etc.]?

[Expected response length: 2 Paragraphs]

At the end of the scenario in part one, I belive that this is not yet considered a HiPPAA breach. The Cyber team has identifed that the Ryuk ransomeware is underway. Untill the Cyber team can veriy that the intruders have acquired or viewed the data. What kind of PHI has been acquired, including the types of identifiers and the likelihood of re-identification. Whether the Intruders have used the PHI information or to whom the disclosure was made and to what extent of the protected health information has been mitigated. The Cyber team needs to locate and lockdown the infected systems. Than contain the ransomeware from expanding.

At this point I would notify all offices and facilites to switch to downtime procedure immediately. Untill we can Prove that the intruders have indeed breached our protected health information. If they have I would than provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, We than must notify covered entities if a breach occured at or by the business associate.

Section 2

A. Navigate to the Instructions page to access Section 2 Scenario.

B. Answer the following questions:

1. During the time it takes to plan actions, the following question needs to be addressed:

2. Should an outside forensics firm be engaged?

3. Should the FBI be called in at this time? Consider the pros and cons of calling them in or not.

[Expected response length: 3-4 Paragraphs]

I belive we will require the assistance of a forensic firm in order to conduct a forensic investigation and prepare an expert report on its findings. They may also provide legal advice. The forensic analysis is crucial for counsel in understanding what occurred and formulating legal strategy relating to potential litigation and breach notification issues.

If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. The FBI has explicitly stated that companies that suffer data breaches should be treated as victims. The agency does not come in with raid jackets and shut down operations, nor are they looking to gather information in order to share it with other regulatory agencies.

The FBI offers guidance on when to get the authorities involved, which includes reporting to the agency in a timely way if a cyber incident Involves significant loss in data, system availability, or control of systems, if the incident Impacts a large number of victims, if the incident Indicates unauthorized access to or malicious software on critical information technology systems, weather the incident Affects critical infrastructure or core government functions, if the incident Impacts national security, economic security, or public health and safety.

After a cyber incident is discovered, the FBI can offer more resources to the victim than they otherwise would have had. Tapping into those resources can help stop the damage, mitigate reputational losses, and it can help authorities to better do their job in the collective fight against cyber crime. the FBI may be intimately familiar with a particular criminal group’s process so that you are more aware of what you’re dealing with as you go through the response. The FBI might have access to decryption keys that have been successfully used in responding to previous attacks from your attacker. The FBI might be able to deployed a sting operation and arrest the suspect. Engaging the authorities during a cyber incident can invoke what’s called a law enforcement hold during investigations, which prevents a company from disclosing the breach publicly.

Reputational harm is a real thing after a disclosed cyber event. Stock prices drop, consumers react, and it can take a long time for companies to regain trust. When a company is ready to disclose, letting stakeholders know that it is working closely with authorities gives gravity to the company’s incident response. Having the right response during a cyber incident can have a net positive effect from a public perception standpoint.

Section 3

A. Navigate to the Instructions page to access Section 3 Scenario.

B. Answer the following questions:

1. Should the organization just pay the ransom? Explain, addressing:

Is this legal?

Is this ethical? If your answers to these questions differ, explain.

Who do you think should be involved in approval (or disapproval) of such payment?

What if the attacker doesn’t provide the decryption key/protocol after payment?

See: Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments – from Treasury Department

[Expected response length: 3-4 Paragraphs]

Off site backup is intact, last backup was 6 hous ago offsite and are accessible, not encrypted by the ransomware. With all the data intact off site, I wouldn't recomend paying any Ransom. Start Cleaning the infected computers and Devices. Wiping the Laptops and desktop of all infected computers and take the downtime hit to reinstate operations. I would only Pay a ramsom under the advise of the CISA, FBI, and HHS. CISA, FBI and HHS do not recommend paying ransoms. Payment does not guarantee files will be recovered. It may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities.

Facilitating a ransomware payment that is demanded as a result of malicious cyber activities may enable criminals and adversaries with a sanctions nexus to profit and advance their illicit aims. Ransomware payments made to sanctioned persons or to comprehensively sanctioned jurisdictions could be used to fund activities adverse to the national security and foreign policy objectives of the United States. Such payments not only encourage and enrich malicious actors, but also perpetuate and incentivize additional attacks. There is no guarantee that companies will regain access to their data or be free from further attacks themselves. For these reasons, the U.S. government strongly discourages the payment of cyber ransom or extortion demands.

OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if such person did not know or have reason to know that it was engaging in a transaction that was prohibited under sanctions laws and regulations administered by OFAC. OFAC strongly encourages all victims and those involved with addressing ransomware attacks to report the incident to CISA, their local FBI field office, the FBI Internet Crime Complaint Center, or their local U.S. Secret Service office as soon as possible. Victims should also report ransomware attacks and payments to Treasury’s OCCIP and contact OFAC if there is any reason to suspect a potential sanctions nexus with regard to a ransomware payment. In doing so victims can receive significant mitigation from OFAC when determining an appropriate enforcement response in the event a sanctions nexus is found in connection with a ransomware payment

By reporting ransomware attacks as soon as possible, victims may also increase the likelihood of recovering access to their data through other means, such as alternative decryption tools, and in some circumstances may be able to recover some of the ransomware payment. Additionally, reporting ransomware attacks and payments provides critical information needed to track cyber actors, hold them accountable, and prevent or disrupt future attacks.

Section 4

A. Navigate to the Instructions page to access Section 4 Scenario.

B. Answer the following questions:

1. How do you ensure the backups aren’t also infected?

Before you restore from a backup, verify that it is free from any malware. You should only restore from a backup if you are very confident that the backup and the device you're connecting it to are clean.

3-2-1 backup rules

The 3-2-1 backup strategy is made up of three rules: Three data copies. Three copies of all critical data should be made on a regular basis -- daily or more frequently -- including the original data and at least two backups. Two types of storage.

2. How can you make sure the unauthorized actor isn’t in your system anymore?

the best plan of action is to completely wipe all of your storage devices and start afresh, reinstalling everything from the bottom up. This will make sure that there aren’t any traces of ransomware lurking in dark corners, and you’ll have a clean slate on which to restore your data.

3. What are the general steps for recovery from backup? Explain in terms of data recovery objectives as defined in NIST SP 800-34 Rev. 1 (addressed in Practitioner level Knowledge Area Information Security Business Impact Analysis section).

1. Develop the contingency planning policy;

2. Conduct the business impact analysis (BIA);

3. Identify preventive controls;

4. Create contingency strategies;

5. Develop an information system contingency plan;

6. Ensure plan testing, training, and exercises; and

7. Ensure plan maintenance

Based on the information above, what is the minimum value possible for offsite backup's Recovery Point Objective (RPO)? Explain how you arrived at this value.

Recovery Time Objective (RTO). RTO defines the maximum amount of time that a system

resource can remain unavailable before there is an unacceptable impact on other system resources,

supported mission/business processes, and the MTD. Determining the information system resource

RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.20

When it is not feasible to immediately meet the RTO and the MTD is inflexible, a Plan of Action and

Milestone should be initiated to document the situation and plan for its mitigation.

Discuss whether beginning restoration of systems at this time (52 hours after the ransomware encrypted systems) should be within the Maximum Tolerable Downtime (MTD) for Regional Hospital.

Maximum Tolerable Downtime (MTD). The MTD represents the total amount of time the system

owner/authorizing official is willing to accept for a mission/business process outage or disruption and

includes all impact considerations. Determining MTD is important because it could leave

contingency planners with imprecise direction on (1) selection of an appropriate recovery method,

and (2) the depth of detail which will be required when developing recovery procedures, including

their scope and content

4. How can you restore systems without destroying evidence for the forensic firm? In other words, what steps must be taken to preserve the evidence from systems before they are restored?

Keep at least one copy of your original data on a separate disk than the one in the computer you're backing up. Store your data backup on a separate site. Verify your backup data isn't corrupted, invalid, or incorrect before disaster strikes.

Properly secure the evidence by placing it in a paper bag or envelope. Close, seal, or tape the paper bag or envelope. The examiner must initial, date, and time across the sealed area. Label the bag or envelope with the patient's identifying information.

[Expected response length: 5 Paragraphs]

Ransomware attacks are most likely to hit during business hours because user actions usually kick them off. We can shut down the system and then restore it from the back up off site. This will temporarily wipe out all of that day’s transactions. However, this is better than nothing and will ensure that the ransomware program is wiped out. Once the system is back, and the users have most of their data, we have time to look through the offsite incremental backup, compare file versions and see where we can provide a more up-to-date version of specific files. Hopefully the CyberTeam follwed the 3-2-1 backup rules.

The 3-2-1 backup strategy is made up of three rules: Three data copies. Three copies of all critical data should be made on a regular basis -- daily or more frequently -- including the original data and at least two backups. Two types of storage. To make sure the unauthorized actor isn’t in our system anymore, the best action is to completely wipe all of the storage devices and start afresh, reinstalling everything from the bottom up. This will make sure that there aren’t any traces of ransomware lurking in dark corners, and we'll have a clean slate on which to restore our data.

The general steps for recovery from backup as defined in NIST SP 800-34 Rev. 1 are :

1. Develop the contingency planning policy;

2. Conduct the business impact analysis (BIA);

3. Identify preventive controls;

4. Create contingency strategies;

5. Develop an information system contingency plan;

6. Ensure plan testing, training, and exercises; and

7. Ensure plan maintenance

The minimum value possible for offsite backup's Recovery Point Objective (RPO) should be as close to Zero as possible to minimize the overall risk to both the business and their customers. An application that handles financial transactions with a non-zero RPO could lose deposits or transactions. A reservation system could lose customer reservations. Even worse, losing patient data in real-time healthcare systems could directly impact patient safety.

Thats the goal at least but hard to achieve. I arrived at this value because the last offsite backup was 6 hours before the incident, Recovery Time Objective (RTO). RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes although that wasnt the case in this scnario it took the Incendent Response team alot longer than 6 hours.

Preserving the evidence from systems before they are restored without destroying evidence for the forensic firm by Keeping at least one copy of your original data on a separate disk than the one in the computer you're backing up. Store your data backup on a separate site. Properly secure the evidence by placing it in a paper bag or envelope. Close, seal, or tape the paper bag or envelope. The examiner must initial, date, and time across the sealed area. Label the bag or envelope with the patient's identifying information.

Section 5

A. Navigate to the Instructions page to access Section 5 Scenario.

B. Answer the following questions:

1. Who must be notified and when? [The patient or their personal representative, HHS, consumer reporting agencies, the media, etc.? State data breach requirements can require more but not less than the Federal requirements.] Hint: You get these numbers from the forensics report.

Note: Acquisition, access, use, or disclosure of unsecured protected health information in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach unless the Covered Entity or Business Associate can demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment. Unfortunately, “compromise” is not well defined.

<https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>

For more information on breach notifications: <https://www.bakerlaw.com/BreachNotificationLawMap>

[Expected response length: 2 Paragraphs]

The Hospital must comply with the applicable breach notification provisions. Five States, Kentucky ( 5,961 ), Massachusetts (9), Ohio (3,657), Pennsylvania (426), West Virginia (4,963) each have their own requirements and who to contact:

Kentucky - Notice to the Attorney General or State Agency is not required, but if more than 1,000 persons must be notified at one time, then the information holder must notify all consumer reporting agencies.

Notice is not required within an explicit number of days, but it must be made expediently and without unreasonable delay. If more than 1,000 persons must be notified at one time, the information holder must notify, without unreasonable delay, all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis.

Massachusetts - The Attorney General and the director of consumer affairs and business regulation must be notified regarding a breach. Even tho only 9 PHI was breached.

Notice is required within seven business days after a law enforcement agency determines that the notification will not compromise a criminal investigation. If the breach of security includes a social security number, the person or agency must contract with a third party to offer each resident whose social security number was disclosed or is reasonably believed to have been disclosed credit monitoring services at no cost for a period of not less than 18 months.

Ohio - If more than 250 Ohio residents are affected, notice to the Ohio Department of Insurance must be made within 15 days of discovering a “loss of control” of a policyholder’s personal information if the covered entity holds a license or certificate of authority from the superintendent of insurance.

If more than 1,000 residents are affected, consumer reporting agencies must be notified of the timing, distribution and content of the disclosure given to the residents of the state.

Notice must be provided in the most expedient time possible but not later than 45 days following discovery or notification of a breach. If more than 1,000 residents are affected, consumer reporting agencies must be notified of the timing, distribution and content of the disclosure given to the residents of the state. An obligation to notify consumer reporting agencies does not permit delaying notification to the affected residents or owner of the data.

Pennsylvania - Notice to the Attorney General or State Agency is not required.

If an entity notifies more than 1,000 individuals at one time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution and number of notices.

Notice is not required within an explicit number of days, but notice must be made without unreasonable delay. When an entity notifies more than 1,000 persons at one time, the entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, of the timing, distribution and number of notices.

West Virginia- Notice to the Attorney General or State Agency is not required. However, if more than 1,000 individuals must be notified at one time, then all consumer reporting agencies must be notified.

Notice is not required within an explicit number of days, but it should be provided in the most expedient time possible and without unreasonable delay. If an entity is required to notify more than 1,000 persons of a breach, the entity shall also notify, without unreasonable delay, all consumer reporting agencies of the timing, distribution and content of the notices. The entity must not provide to the consumer reporting agency the names or other personal identifying information of breach notice recipients.

Section 6

A. Navigate to the Instructions page to access Section 6 Scenario.

B. Answer the following questions:

1. What are 5 recommendations (in priority order) that you would suggest the organization take to avoid/mitigate similar attacks and why?

2. Which area(s) of the NIST Cybersecurity Framework (CSF) do you think needs to be reinforced and why?

[Expected response length: at least 2 pages]

After reading and considering all the details that have come to light about this incident I would recomend the 5 suggestion in order of priority:

1. Enforce Signed Software Execution Policies, Use a modern operating system that enforces signed software execution policies for scripts, executables, device drivers, and system firmware. Maintain a list of trusted certificates to prevent and detect the use and injection of illegitimate executables. Execution policies, when used in conjunction with a secure boot capability, can assure system integrity. Application Whitelisting should be used with signed software execution policies to provide greater control. Allowing unsigned software enables threat actors to gain a foothold and establish persistence through embedded malicious code.

2. Update and Upgrade Software Immediately, Apply all available software updates, automate the process to the extent possible, and use an update service provided directly from the vendor. Automation is necessary because threat actors study patches and create exploits, often soon after a patch is released. These “N-day” exploits can be as damaging as a zero-day. Vendor updates must also be authentic; updates are typically signed and delivered over protected links to assure the integrity of the content. Without rapid and thorough patch application, threat actors can operate inside a defender’s patch cycle.

3. Transition to Multi-Factor Authentication, Prioritize protection for accounts with elevated privileges, remote access, and/or used on high value assets. Physical token-based authentication systems should be used to supplement knowledge-based factors such as passwords and PINs. Organizations should migrate away from single factor authentication, such as password-based systems, which are subject to poor user choices and susceptible to credential theft, forgery, and reuse across multiple systems

4. Actively Manage Systems and Configurations, Take inventory of network devices and software. Remove unwanted, unneeded or unexpected hardware and software from the network. Starting from a known baseline reduces the attack surface and establishes control of the operational environment. Thereafter, actively manage devices, applications, operating systems, and security configurations. Active enterprise management ensures that systems can adapt to dynamic threat environments while scaling and streamlining administrative operations.

5. Continuously Hunt for Network Intrusions, Take proactive steps to detect, contain, and remove any malicious presence within the network. Enterprise organizations should assume that a compromise has taken place and use dedicated teams to continuously seek out, contain, and remove threat actors within the network. Passive detection mechanisms, such as logs, Security Information and Event Management (SIEM) products, Endpoint Detection and Response (EDR) solutions, and other data analytic capabilities are invaluable tools to find malicious or anomalous behaviors. Active pursuits should also include hunt operations and penetration testing using well documented incident response procedures to address any discovered breaches in security. Establishing proactive steps will transition the organization beyond basic detection methods,enabling real-time threat detection and remediation using a continuous monitoring and mitigation strategy.

The intrusion started from a eMail attachment from an employee computer, If It had shut down and quarantined attachments and stopped all users from installing any software on their workstations, It could have stopped the intrusion at the gate. Updating all workstations would have caught the trickbot before the Ryuk could have been allowed access. Multi-Factor Authentication could have informed the owner of the workstation that someone is trying to log-in the Computer. Cyber Security team could've also been scaning and looking for data and traffic flows more often.

The area(s) of the NIST Cybersecurity Framework (CSF) I think that needs to be reinforced are:

Within the Identify Section :

Document information flows – It’s important to not only understand what type of information your enterprise collects and uses, but also to understand where the data is located and flows, especially where contracts and external partners are engaged.

Establish policies for cybersecurity that include roles and responsibilities – These policies and procedures should clearly describe your expectations for how cybersecurity activities will protect your information and systems, and how they support critical enterprise processes. Cybersecurity policies should be integrated with other enterprise risk considerations (e.g., financial, reputational).

Identify threats, vulnerabilities, and risk to assets – Ensure risk management processes are established and managed to ensure internal and external threats are identified, assessed, and documented in risk registers. Ensure risk responses are identified and prioritized, executed, and results monitored. Signature-based protections must remain up to date, such as anti-virus and other signature-based protections. Up-to-date antivirus protections can safeguard your organization against known malware that has been seen before and has an existing and recognized signature. Two key components to consider are threat extraction (file sanitization) and threat emulation (advanced sandboxing),” they added. “Each element provides distinct protection, that when used together, offer a comprehensive solution for protection against unknown malware at the network level and directly on endpoint devices.

Within the Protection Section :

Manage access to assets and information – Create unique accounts for each employee and ensure that users only have access to information, computers, and applications that are needed for their jobs. Authenticate users (e.g., passwords, multi-factor techniques) before they are granted access to information, computers, and applications. Tightly manage and track physical access to devices. Access management is critical to minimizing the potential impact of ransomware, which ensures users only have access to data and resources necessary to execute their job function.

Protect sensitive data – If your enterprise stores or transmits sensitive data, make sure that this data is protected by encryption both while it’s stored on computers as well as when it’s transmitted to other parties. Consider utilizing integrity checking to ensure only approved changes to the data have been made. Securely delete and/or destroy data when it’s no longer needed or required for compliance purposes.

Conduct regular backups – Many operating systems have built-in backup capabilities; software and cloud solutions are also available that can automate the backup process. A good practice is to keep one frequently backed up set of data offline to protect it against ransomware. Backups should be automated if possible to avoid relying on employees to remember to routinely execute the process on their own.

Securely protect your devices – Consider installing host-based firewalls and other protections such as endpoint security products. Apply uniform configurations to devices and control changes to device configurations. Disable device services or features that are not necessary to support mission functions. Ensure that there is a policy and that devices are disposed of.

Manage device vulnerabilities – Regularly update both the operating system and applications that are installed on your computers and other devices to protect them from attack. If possible, enable automatic updates. Consider using software tools to scan devices for additional vulnerabilities; remediate vulnerabilities with high likelihood and/or impact.

Train users – Regularly train and retrain all users to be sure that they are aware of enterprise cybersecurity policies and procedures and their specific roles and responsibilities as a condition of employment. Employee education is also crucial, given the most common infection method remains spam and phishing emails. Research has shown phishing education can drastically reduce the healthcare’s cybersecurity risk. It’s also important to encourage employees to report any suspicious activity to the security team.

DeteWithin the Detect Section :

Test and update detection processes – Develop and test processes and procedures for detecting unauthorized entities and actions on the networks and in the physical environment, including personnel activity. Staff should be aware of their roles and responsibilities for detection and related reporting both within your organization and to external governance and legal authorities.

Maintain and monitor logs – Logs are crucial in order to identify anomalies in your enterprise’s computers and applications. These logs record events such as changes to systems or accounts as well as the initiation of communication channels. Consider using software tools that can aggregate these logs and look for patterns or anomalies from expected network behavior.

Know the expected data flows for your enterprise – If you know what and how data is expected to flow for your enterprise, you are much more likely to notice when the unexpected happens – and unexpected is never a good thing when it comes to cybersecurity. Unexpected data flows might include customer information being exported from an internal database and exiting the network. If you have contracted work to a cloud or managed service provider, discuss with them how they track data flows and report, including unexpected events.

After this breach everyone knows the Impact this threat cause, I hope everyone will continue to Seek help and Communicating information on the event.

Within the Respond Section :

Ensure response plans are tested – It’s even more important to test response plans to make sure each person knows their responsibilities in executing the plan. The better prepared your organization is, the more effective the response is likely to be. This includes knowing any legal reporting requirements or required information sharing.

Ensure response plans are updated – Testing the plan (and execution during an incident) inevitably will reveal needed improvements. Be sure to update response plans with lessons learned.

Coordinate with internal and external stakeholders – It’s important to make sure that your enterprise’s response plans and updates include all key stakeholders and external service providers. They can contribute to improvements in planning and execution.

Within the Recover Section :

Communicate with internal and external stakeholders – Part of recovery depends upon effective communication. Your recovery plans need to carefully account for what, how, and when information will be shared with various stakeholders so that all interested parties receive the information they need but no inappropriate information is shared.

Ensure recovery plans are updated – As with response plans, testing execution will improve employee and partner awareness and highlight areas for improvement. Be sure to update recovery plans with lessons learned.

Manage public relations and company reputation – One of the key aspects of recovery is managing the enterprise’s reputation. When developing a recovery plan, consider how you will manage public relations so that your information sharing is accurate, complete, and timely – and not reactionary.

All of this can't be achieved without a Strong Cybersecurity Workforce. A skilled cybersecurity workforce is needed to meet the unique cybersecurity needs of critical infrastructure. There is a well-documented shortage of general cybersecurity experts; however, there is a greater shortage of qualified cybersecurity experts who also have an understanding of the unique challenges posed to particular parts of critical infrastructure. As the cybersecurity threat and technology environment evolves, the cybersecurity workforce must continue to adapt to design, develop, implement, maintain and continuously improve the necessary cybersecurity practices within critical infrastructure environments. Various efforts, including the National Initiative for Cybersecurity Education (NICE), are currently fostering the training of a cybersecurity workforce for the future, establishing an operational, sustainable and continually improving cybersecurity education program to provide a pipeline of skilled workers for the private sector and government. Organizations must understand their current and future cybersecurity workforce needs, and develop hiring, acquisition, and training resources to raise the level of technical competence of those who build, operate, and defend systems delivering critical infrastructure services

Refences:

[www.nsa.gov](http://www.nsa.gov/)

<https://www.cisa.gov/>

[https://home.treasury.gov](https://home.treasury.gov/)

<https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>

<https://www.nist.gov/>

<https://www.ncsc.gov.uk/>

<https://www.bakerlaw.com/>

<https://woodruffsawyer.com/>

<https://www.hodgsonruss.com/>