QUESTION 11:

WHAT IS MY PLAYBOOK IF I HAVE A CYBERSECURITY INCIDENT?

"Companies should be thinking about the legal and managerial decisions that the CEO, the COO and the board will need to make in that kind of crisis situation."

– Michael Vatis, founding Director of the FBI's National Infrastructure Protection Center

"I have been investigating a large number of failed logins on the Microsoft Hyper-V server. The accounts that were attempting to log in were our managed service provider Service Admin Account and your Domain Admin account. Due to the volume of failed attempts, it does appear that the attempts are coming from an outside source. My company recommends that you reach out to a Security Firm to have your network investigated for a possible breach. Please let me know if you would like a recommendation."

I couldn't believe what I was reading. A new client I had started working with only weeks earlier forwarded me the email above from their computer network management provider. The owner of the business was

concerned, and he had good reason to be. This was a healthcare company, and HIPAA breaches are serious. I had come onboard as their part-time CISO the month before, and the vendor that manages their network had kicked this ball squarely into my court. I had to figure out what to do and fast.

My priorities were simple:

1. Alert my client's executive team about the situation.
2. Determine if this is or is not a real hacking attempt.
3. If it is a real hacking attempt, determine how it is occurring.
4. Assess if the hack was successful in any way. Was any damage done? Was any data accessed?
5. If the hack was unsuccessful, terminate the hacker's access immediately.
6. If the hack was successful, start making calls to my client's CEO, their cybersecurity insurance carrier, a third-party company that specializes in breach remediation, and my client's attorney.
7. Follow-up with root-cause analysis and recommend preventive measures.

After calling the business owners and the company's CEO to let them know of the issue, I began working with their technology team to review thousands of failed login attempts. Over 500 per minute were being processed, and it was obvious that a classic dictionary password-cracking attempt was underway. I breathed a tiny sigh of relief to see that it had only started several hours earlier and appeared to be moving ahead at full steam, which meant that the bad guys had most likely not yet been successful at cracking an administrator-level password.

Now to figure out where it was coming from. The internal network showed no signs of trouble, and no unusual logins were found on the Virtual Private Network (VPN) portal. That left an Internet-based intruder as the only option. As soon as we put the pieces together, it was obvious what had gone wrong. A firewall configuration change from the night before had accidentally opened up several holes (called ports) from the Internet to an internal server (mistake #1). One of those ports, number 3389, was a common port used to remotely control servers (mistake #2). The server in question had not been configured to use a non-standard port for that remote-control functionality (mistake #3). Hackers worldwide that are scanning the Internet for computers that respond on port 3389 because they are an easy target.

This client didn't have a playbook on what to do when a cybersecurity incident is suspected, so we had to make it up as we went.

I had the offending ports in the firewall closed immediately. The login attempts stopped.

My blood pressure began to return to a more reasonable level.

The example above is real, and while it represents the best possible outcome of a cybersecurity incident, I used it here to make a number of points. This client didn't have a playbook on what to do when a cybersecurity incident is suspected, so we had to make it up as we went.

Doing so took extra time and might have led us to miss obvious steps.

- The executive management team did not have documented steps to take in their various departments to help bring operations back online if the hack had been successful, nor did they have procedures to follow if it was determined that any HIPAA protected data had been compromised.

- Their IT services vendor wasn't well trained in how to help us get to the bottom of the technical issues quickly, which lengthened the incident by hours.
- The client didn't have a checklist of whom to call when as a cybersecurity incident unfolded, which made my phone number the only number they thought to use.

What if I was unavailable when this took place? From a system design standpoint, I was a "single point of failure"—that is, if I wasn't available, the incident response process broke down. Not good. In a nutshell, we didn't yet have our act together, and it showed.

After an incident occurs, your company will be judged on the following criteria:

1. Did your company take all actions to prevent the incident that one would expect of a prudent organization?
2. Did your company respond to the incident using procedures that one would expect of a prudent organization?
3. Are there any ways that the media can portray your actions around steps 1 and 2 to make your company appear to be culpable or incompetent? If true, expect that they will. It attracts more readers to their publication.

A robust playbook that includes the involvement and actions of the President & CEO, Chief Legal Counsel, Chief Operating Officer, VP of Sales, VP of Human Resources, VP of Communications, Chief Security Officer, and the CIO and CISO will do immeasurable good in your ability to respond to an incident.

An incident response playbook needs several key elements to be effective. It must:

- Identify who in your organization has the authority to declare a cybersecurity incident. Who can initiate the playbook?
- Spell out how much money that person can authorize to be spent to have an incident investigated or remediated. If the CFO and CEO are out of town, this person needs to understand the parameters he/she can work within until the CFO or CEO can be reached.
- Have a list of the types of scenarios that it is designed to cover. Examples include the loss of sensitive data, a ransomware attack, the loss of a critical system, natural disasters, law enforcement contacting your organization about a warrant or subpoena, law enforcement contacting your organization about a suspected cybersecurity incident that you are unaware of, the loss of the use of one or more of your sites due to a natural disaster or because of other issues (such as a crime taking place in the building and the police barring your employees from entering the premises).
- Have a call tree that includes which people or groups to call when an incident takes place. See Question 7 for more on this point.
- Define the parameters under which law enforcement should be involved in a suspected breach, and the people or groups responsible for making the decision on when to bring in law enforcement.
- Include who can speak to the media about a cybersecurity incident, and what those who are not authorized to speak to the media should say if they are approached by a reporter.

- List all of your critical systems, the location of the data in those critical systems, and the location of the backups of the data for those systems.
- Have the maximum allowable downtime of each of your systems. This is called an RTO, or Recovery Time Objective. While it would be great if every system was always 100% up and running, that isn't realistic. Your mission-critical ERP system is usually much more important to your business than the computer monitors that display promotional videos in your lobby, for example. A realistic RTO for your ERP system may be 4 hours or even less. For those displays in the lobby, an RTO of a week or more may be acceptable.
- Have lists of the age of backup data for each system. You need a maximum amount of acceptable data loss per system, and your backup methodology for each system should be chosen based on that maximum, called an RPO, or Recovery Point Objective. Much like the RTO, it would be fantastic if every backup system had up-to-the-minute copies of your data, but for most of us, that is prohibitively expensive. Typically, three schools of thought exist about RPO's:

    1. You may have a regulatory or contractual obligation that spells out your RPO. In that situation, it's a moot point for you to come up with your own.
    2. You may be a large enough organization so that it is worthwhile to go through each system and have a discussion on the impact of losing one hour's worth of data, 2 hour's data, 4 hour's data, and one entire business day. Then get rough costs on backup solutions

for each RPO. Make your business decision for each system by taking those data points into account.

3. Make your RPO one business day for everything, run nightly backups on everything, and move on with life.
   The best answer on RPOs for your organization depends on your situation.

- Cover the general incident-response process. While every scenario is different, this process normally follows these steps: preparation, detection/analysis, containment, eradication, recovery, incident closure/root-cause analysis, and preventative measures.
- Be reviewed on a frequent basis. These plans get stale quickly, and need to be reviewed whenever a significant change in your organization takes place.

If the above points are reviewed as a group, an interesting trend emerges. *Most of them are non-technical*. The majority are operational and financial in nature. That is a critical misstep in many incident response plans. If your technology team manages your incident response plan, they are making business and financial decisions that should be made by CEOs and COOs and CFOs and legal counsel. Your technology team should be advising a non-technology executive—often the COO or CEO—on any technology issues that directly impact the plan, but a non-technical executive should own it.

Your incident response plan needs to be tested. This is too important to be left to guesses.

Above all, your incident response plan needs to be tested. Unless you have tried out an incident response procedure, you're only able to guess if it will work. This is too important to be left to guesses. Question 12 deals with incident response plans in more detail, but it's worth repeating here.

The companies I have worked with that get their playbooks right have a distinct difference from those that do not: playbooks that are used often are much more useful than those that are rarely touched. While this is easier for larger companies to accomplish than smaller ones, it is often the smaller companies that are more in need of an up to date incident response plan when issues arise.

The takeaway messages from this section are easy to list:

- Your company needs an incident response playbook.
- The incident response playbook should be owned by a non-technical member of your executive team. Most decisions in the playbook are operational, financial or communications specific, not technology specific. Technology leadership should play a supporting role, not a primary role.
- Your company needs to periodically test your incident response capabilities.
- Your company needs to update the playbook from lessons learned as a result of tests, whenever significant changes occur to the operational or technical aspects of the company, or when merger/acquisition activity occurs.

QUESTIONS TO EXPLORE this topic further with your company's leaders:

- How do we test our incident response playbook?
- How often do we test it?
- What did we learn from our last test?