PREPARING YOUR CYBERSECURITY BREACH RESPONSE

Authored by:
Colin Konschak, FACHE, Divurgent
Shane Danaher, MBA, Divurgent

INTRODUCTION

If you're in healthcare, your organization is an especially attractive cybercrime target because of the value of the sensitive information you are trying to safeguard, and how lax cybersecurity generally is in your industry. Recent studies show your costs of being successfully targeted are rising, not falling as they are in other industries. In addition to being in the healthcare sector, your location is also a factor in the high cost of breach response. Doing business in the United States means you are located where notification and post-data breach response costs are the highest in the world. (Ponemon Institute, 2017)

A major reason for these high costs is that the healthcare industry is highly regulated and under a great deal of scrutiny, especially when it comes to safeguarding personally identifiable information (PII) and protected health information (PHI). In a previous whitepaper in this 10-part series on cybersecurity titled, "HIPAA and the Intersection of Cybersecurity in Healthcare," we detailed the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Health Information for Economic and Clinical Health Act (HITECH) and other federal regulations that govern protection of sensitive information. We also detailed the compliance responsibilities of covered entities and their business associates under HIPAA's Privacy and Security Rules, and the Breach Notification Rule.

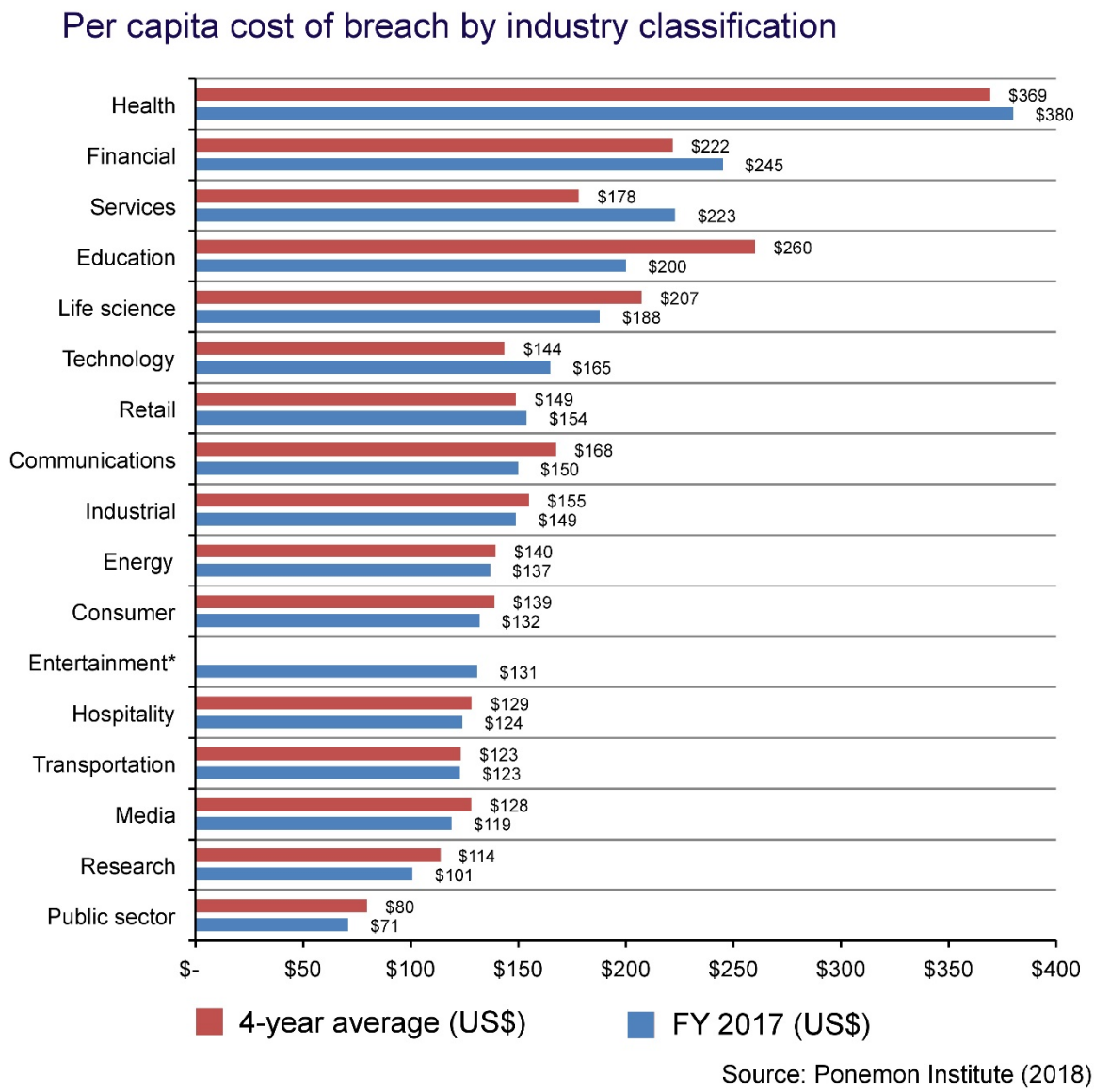
In preparing for a cybersecurity breach, which leaders in the healthcare industry should consider as inevitable, not only federal regulations have to be considered, but state data breach laws as well. While federal law generally pre-empts state laws when the state laws are less stringent, covered entities must comply with the state breach notification laws to the extent that they exceed the notification requirements in HIPAA. Due to the myriad of state laws and requirements, it is possible a security incident that does not trigger a breach under HIPAA may trigger a breach requiring notification under state law.

In this whitepaper, we focus on ways to help ensure your organization has a well-developed plan to respond quickly and effectively to a cybersecurity breach involving the theft or ransom of sensitive information.

CONSIDERING THE COSTS OF BREACHES

In a 2017 Ponemon Institute study that analyzed the costs of breaches globally in several business sectors, researchers found that the average cost worldwide of a data breach was $3.62 million, which is down 10 percent from previous years. The average cost for each lost or stolen record containing sensitive information also significantly decreased from $158 in 2016 to $141 in 2017. Not so in the healthcare sector, where the average data breach costs have risen to $380 per record—more than 2.5 times the overall average cost. (See Figure 1). That is a 12-percent higher cost per record than in the next highest sector, financial services, which one might assume would have higher costs and be a bigger target. (Ponemon Institute, 2017).

Figure 1: Per Capita Cost of Breaches: 2017 and Four-Year Average



Source: Ponemon Institute (2018)

THE PROBLEM WITH BREACH RESPONSE PLANS

If you have a breach response plan, no matter what industry you are in, chances are it doesn't exactly help you sleep soundly at night. In its 2018 (fifth annual) study on data breach preparedness, Ponemon Institute surveyed 624 U.S. executives and staff employees who work primarily in privacy, compliance and IT security. When asked whether they believe their organizational data breach response plan is highly effective, only 19 percent, or 119 of them,

replied in the affirmative. Of these, 56 percent had already experienced a breach in 2017, which is an increase of 52 percent last over the previous year, and 70 percent of those organizations reported multiple breaches (Ponemon Institute, 2018).

The Ponemon study also noted two factors that are particularly relevant to the healthcare sector that complicate data breach preparedness and so should be incorporated into plans. These are the increasing risk of data breaches due to:

- Unsecured Internet of Things (IoT) devices in the workplace (use of connected devices is growing rapidly in hospitals and healthcare systems)
- Ransomware and phishing attacks (these are the most common attacks in healthcare)

GETTING STARTED WITH YOUR PLAN

As cybersecurity attacks and their costs have quickly multiplied in this decade, organizations in many business sectors have been developing breach response plans. One might believe that confidence in data breach response plans would be drastically improving over the years as more organizations in all business sectors create and implement such plans. However, Figure 2 below shows only minor improvements.

Figure 2: Perception of Data Breach Response Plan Effectiveness

Source: Ponemon Institute (2018).

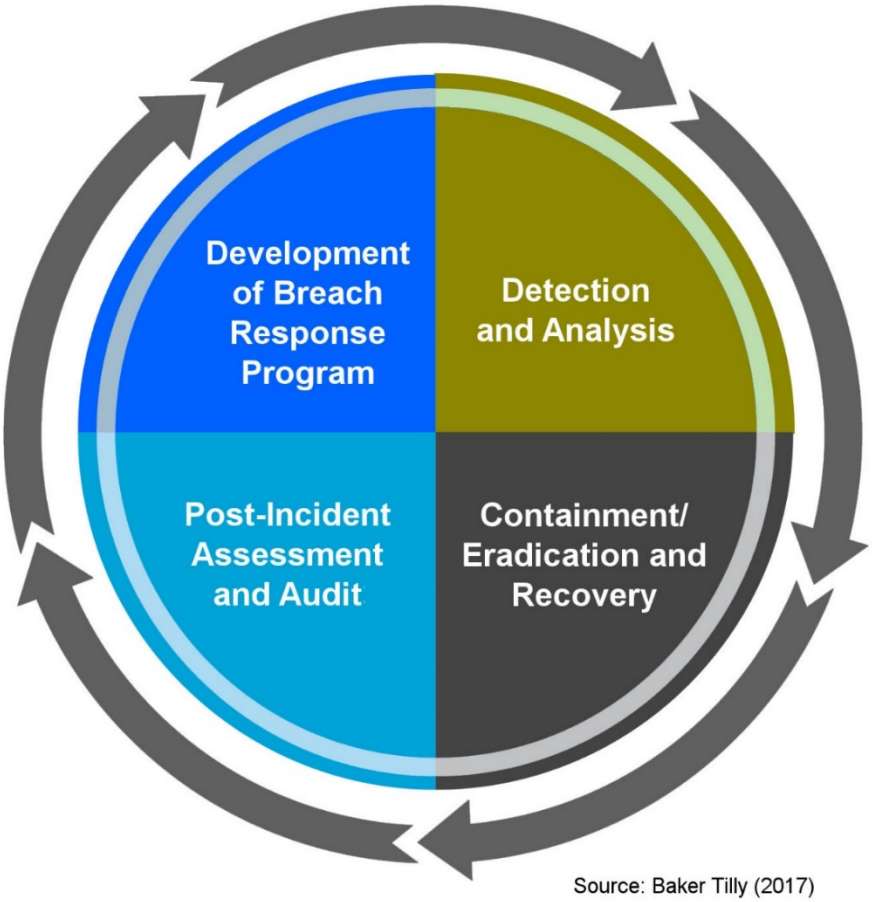
So how does an organization create a data breach response plan that it can have confidence in? Properly preparing your people and your organization to comply in the event of a breach is an intensive process, but it is one that may reap the ultimate positive outcome—not experiencing a breach in the first place. Just as with a disease, understanding the underlying causes is one of the greatest steps toward a cure. Or better yet, prevention.

This understanding of where your organization is at in terms of cybersecurity is the starting point for an effective plan. Most organizations refer to the result of these efforts as their data breach response plans. However, the best kind of data breach response plan should look more like a preparedness program, rather a plan to react to inevitable harm. Accounting/advisory firm Baker Tilly recommends the four-element approach to breach response shown below in Figure 3 (Baker Tilly, 2017).

So how does an organization create a data breach response plan that it can have confidence in? Properly preparing your people and your organization to comply in the event of a breach is an intensive process, but it is one that may reap the ultimate positive outcome—not experiencing a breach in the first place. Just as with a disease, understanding the underlying causes is one of the greatest steps toward a cure. Or better yet, prevention.

This understanding of where your organization is at in terms of cybersecurity is the starting point for an effective plan. Most organizations refer to the result of these efforts as their data breach response plans. However, the best kind of data breach response plan should look more like a preparedness program, rather a plan to react to inevitable harm. Accounting/advisory firm Baker Tilly recommends the four-element approach to breach response shown below in Figure 3 (Baker Tilly, 2017).

Figure 3: Elements of Breach Preparedness



Source: Baker Tilly (2017)

In developing the breach response program, Baker Tilly recommends that the eight following considerations be addressed:

1. Create an incident response team
2. Designate a responsible executive
3. Inventory the monitoring tools on your systems
4. Identify the signs of a potential breach
5. Establish a protocol if a breach is suspected
6. Define reporting and notification processes
7. Define recovery procedures
8. Test and refine the response plan

PREPARE YOUR WRITTEN RESPONSE PLAN

In order to develop an effective written response plan, a healthcare organization must first identify its data and data collection and storage practices, examine its third-party relationships, and determine who administers its related privacy and security policies and procedures, and how

those policies and procedures are administered. At the outset of embarking on this process, a healthcare organization must define what it considers to be "personal information." The definition may, and likely should, be broader than just healthcare information. For example, personal information can include first initial or first name and last name, address, telephone number, email address, Social Security number, birth date, driver's license number, passport number, credit card number, financial account number, consumer credit reports, employee background checks and credit reports. A sufficiently broad definition will enable the healthcare organization to better identify potentially sensitive data.

While a form, or off-the-shelf, plan may be tempting, every organization is different and each operates in a distinct and unique manner. In order for a response plan to be effective, it must be tailored for, and specific to, your organization. The response plan serves as your organization's map in the event an actual incident or breach occurs. The following questionnaire, and an organization's response, can serve as the starting point for the creation of a response plan.

QUESTIONS FOR LAYING THE FOUNDATION OF YOUR RESPONSE PLAN

1. ***Who will lead the breach response team?*** When a cyberattack occurs, its effects reverberate throughout the organization, touching many individuals and functions. Your written plan must designate a responsible executive (along with a backup) who will serve the team leader and top decision maker during a possible breach. This person will be a liaison among management, the response team and with external individuals and organizations who are affected. This person should have the authority identify and assign tasks. The team leader and backup are often someone from internal or external legal counsel, or the chief privacy officer.

2. ***Who should serve on the breach response team?*** When identifying these members, the following departments should be considered—in-house/general counsel, privacy/compliance, information technology/security, human resources, communications, and customer relations.

   When creating a plan, consider designating a key person on the team who has experience with the security incident investigation and breach response processes. Someone with this kind of experience can be a valuable asset.

3. ***What are the categories of individuals from whom, or about whom, your organization collects personal information?*** Consider that these categories of individuals go far beyond just patients to include employees, independent contractors and volunteers, website visitors, third-party vendors and business contacts.

4. ***For each category of individual, what types of personal information are collected?*** The scope of personal information collected by a healthcare organization greatly expands when the other categories of individuals mentioned above are considered. Just to name

a few examples, this can include financial information relating to payments for services, personal information about employees and independent contractors, and data collected from individuals who visit the organizational website.

5. ***Do the individuals from whom the organization collects data reside in the United States?*** If the answer to this question is no, and individuals reside outside of the United States, then the organization may be required to comply with certain foreign laws as well. For example, if the person is a European Union citizen, the new General Data Protection Regulation (GDPR), which went into effect in May 2018, covers data protection and privacy for all individuals within the European Union. However, it also addresses the export of personal data outside of the EU. As for U.S. laws, HIPAA will clearly apply, but other laws may be implicated as well. For example, if a healthcare organization performs criminal background checks on potential employees, then the Fair Credit Reporting Act may also apply.

6. ***In what formats does the organization store the personal information it collects? Paper, electronic, backup tapes, portable media?*** It is vital not to overlook any format that carries sensitive data in your organization, because they are all vulnerable to breach and theft.

7. ***Does your organization encrypt personal information that is stored electronically? Is encryption applied to information in databases and on backup tapes, portable media and portable devices, such as laptops and mobile devices?*** The Department of Health and Human Services (HHS) recognizes encryption as a safe harbor. Although healthcare organizations are not required to use encryption, PHI that has been secured in accordance with the most current HHS guidance is not covered by the Breach Notification Rule.

8. ***Does the organization encrypt the transmission of personal information? If so, is the encryption applied to all, or only certain types, of personal information being transmitted?***

9. ***What access controls do you have in place?***

10. ***Does the organization monitor and limit access to databases containing personal information? If so, to whom? Is that process documented? Are access rights periodically reviewed?*** Keep in mind that the answers to this question and the previous one can reveal vulnerabilities that lead to a highly significant opportunities for improvement when it comes to keeping cyber criminals out of your systems.

11. ***Does the organization utilize logging that would enable it to identify who accessed files and records?***

12. ***Does the organization use third parties to collect, store, transmit or process data?*** These third parties need to be identified because they need to be part of your organization's breach response plan and other cybersecurity efforts if they are not already. In addition, you need to be part of their notification process in the event they suffer a breach.

13. ***Does the organization have any agreements with third parties that would require the organization to notify that third party in the event of a breach?***

14. ***Who is responsible for developing and implementing privacy and data security policies and procedures?***

15. ***Does the organization have an insurance policy that covers data or security breaches?*** A more detailed discussion of cyber insurance is covered in our whitepaper in this series, titled "Mitigating Cybersecurity Risk: Is Cyber Insurance the Answer?" In general, though, an organization that collects personal information should have a cyber insurance policy. Most general liability policies and errors and omissions policies will not cover a cyber incident or data privacy or security breach.

    As we mentioned earlier, notification and post data breach response costs are highest in the United States. This means these potential costs must be a consideration in what your cyber insurance policy covers. Some examples of some of these costs are:

    - *Notification*—creating contact databases, determining all relevant regulatory requirements, engaging outside experts, postal expenses, email bounce-backs and setting up inbound communication.
    - *Post data breach response*—legal expenses, regulatory interventions, help desk activities, inbound communications, public relations, investigative costs, data and system recovery, and providing identity protection services.

16. ***Does your organization have contact information for appropriate federal and state law enforcement authorities and regulatory agencies? Consumer reporting agencies?*** The written response plan should include contact information for the Federal Bureau of Investigation, state and local law enforcement, and regulatory agencies with authority over the organization.

17. ***Does the organization have a contract with credit/identity-monitoring providers?*** Does the organization have the internal capability to handle communications to and from individuals, such as large-scale mailings and a high volume of calls? If not, does the organization have contracts with call center providers, mailing houses or other providers? Does the organization have a relationship with outside legal counsel with experience in handling data breach incidents and response?

    The response plan should establish emergency contacts and designate outside counsel and experts, such as forensics experts, credit/identity-monitoring providers, call centers and mailing houses.

    Even though the written response plan may designate certain specific third parties (such as legal counsel, forensic experts, credit/identity-monitoring providers, call centers and mailing houses) to contact in the event of a security incident or breach and to engage to provide such relevant services, the insurer is under no obligation to use such designated third parties and the organization may be required to use the third parties as chosen by the organization's insurance company. Organizations should strongly consider

negotiating with the insurance provider to allow the organization to name specific experts within the insurance policy. Without this express, written assurance, the organization may be forced to use other counsel and third parties with whom the client is either unfamiliar or has no ongoing relationship.

For all designated third parties, the organization should negotiate and have in place service contracts that are ready to be activated with a phone call to the third party, notifying that the organization has experienced a security incident. Otherwise, the organization will spend several critical days establishing relationship and accounts that must be set up in advance. This time could be better focused on investigation, mitigation and response efforts within the first several days after a security incident.

18. ***Do you have draft notification letters for individuals? To various federal and state agencies and authorities?*** Federal and state reporting requirements likely include very specific information that must be conveyed in the notice to both the agency itself and to the individuals. Further, state breach notification laws differ, and what you may be required to include in a notification in one state is prohibited in another state. Having drafts of the required notices will save a significant amount of time during the response process and enable you to more quickly and efficiently notify when appropriate.

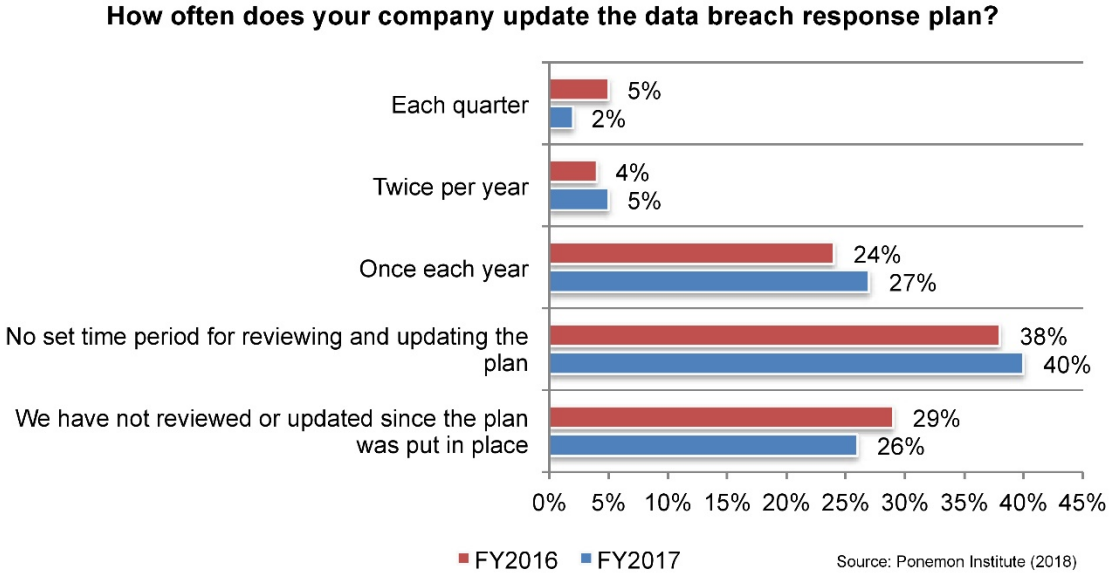
19. ***Do you have prepared media statements and communication plans for your employees?*** Media statements that are prepared in advance, and not under the time constraints and pressure of an active breach situation, are likely to be well thought out and not make assurances that you cannot achieve. Although the statements may need to be slightly altered based on the circumstances, they should be somewhat generic. For example, the statement may convey that you are aware of the situation, you have retained experts to assist you, you have contacted law enforcement and will cooperate with them, and that you will assist the impacted individuals.

The responses to these questions can enable the organization to prepare a written response plan that identifies the response team, contains procedures for analyzing and containing a data breach, includes a plan for notifying affected individuals, and outlines remediation measures to be taken following a data breach.

REVIEWING, UPDATING AND TESTING THE RESPONSE PLAN

Few threats to organizations are evolving as rapidly as cybercrime. That is why your response plan should be reviewed and updated at regular intervals. This intuitively makes sense, but it does not occur often enough. According to Ponemon's 2018 data breach preparedness study, 88 percent of companies reported that they have a data breach response plan. However, as Figure 5 shows, 66 percent of those who have a plan in place do not have an appointed interval for review, or they have a plan that has not been reviewed since it was implemented.

Figure 5: Frequency of Review and Update for Breach Response Plans



If so many of these plans are not regularly reviewed or updated, it is a good bet that many of them are also not regularly practiced, or not practiced at all. The time to test your plan is not when the next incident that occurs. An effective response plan is a practiced response plan. Conducting a breach simulation is an effective way to replicate the challenges of a breach. It will also expose areas of weakness or gaps in the plan that should be addressed. You should practice the plan so that the assembled team has a keen understanding of the process.

Those regular, scheduled tests of the plan will also enable you to make changes to the plan if necessary. If you discover during a test, that one particular aspect did not work as well as planned, then you are able to make changes accordingly, and while you are not under the significant pressure of an actual breach. Also through testing the plan, each member of the team will gain an understanding of his or her specific responsibilities.

When you test your plan, consider enlisting an outside facilitator. This facilitator can run the drill so that each member of the team can focus on his or her responsibilities. The entire response team should be involved in the test run, including your outside team members, such as legal counsel and your forensics firm, because they will ultimately be working together in responding to an actual breach.

The test should include multiple scenarios, address as many “what if” questions as possible and run through multiple scenarios that could take place before, during and after a breach. Allow your team a sufficient amount of time to run through it thoroughly. Once tested, test it regularly. Doing it at six-month intervals will allow your team to have plenty of practice and allow you to make appropriate adjustments in light of internal and external changes and challenges.

RESOURCES FOR MOVING FORWARD WITH YOUR PLAN

All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted breach notification law. To access your jurisdiction's information, go to the National Conference of State Legislatures Security Breach Notification Laws site: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

The HHS Office for Civil Rights (OCR) has published guidance on several important HIPAA Security Rule topics that can help an organization develop all of its cybersecurity programs and data breach response plans, keeping in mind again that state laws and regulations also need to be considered. OCR has published an educational paper series that covers each set of standards and highlights the risk analysis and risk management plan requirements. OCR also publishes a monthly cybersecurity newsletter that spotlights critical topics for consideration by its readers. Many of the OCR resources may be found by starting at the HHS HIPAA for Professionals site at: https://www.hhs.gov/hipaa/for-professionals/index.html.

OCR also promotes use of the various white papers from the National Institute of Standards and Technology (NIST) for the development of one's compliance program. NIST, a part of the Department of Commerce, develops, tests and promotes standards and measurements for the benefit of various industries. Among NIST's many projects is the Cybersecurity Framework, which provides a guide for businesses seeking to adopt and implement a robust cybersecurity program (NIST, 2018). Focused on risk management, the "core" of the Framework focuses on five elements: identify, protect, detect, respond, and recover. NIST and HHS have jointly published a "crosswalk" document that links the Cybersecurity Framework to the HIPAA Security Rule requirements to ensure that, in keeping with NIST's best practices, entities are also aware of their compliance responsibilities. These resources may be found at: https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html. (Office for Civil Rights, 2016).

REFERENCES

Baker Tilly (2017, September 11) *Developing and implementing an effective breach response plan.* Available at http://bakertilly.com/insights/developing-and-implementing-an-effective-breach-response-plan/

Office for Civil Rights. (2016). HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework. Retrieved from https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf?language=es.

Office for Civil Rights. (2018, January 31). *Enforcement Highlights*. Available at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html?language=es.

Ponemon Institute. (2017). *Cost of Data Breach Study: Global Overview*. Available at: https://www.ibm.com/security/data-breach/.

Ponemon Institute. (2018). *Fifth Annual Study: Is Your Company Ready for a Big Data Breach?* Sponsored by Experian. Available at: http://www.experian.com/data-breach/2018-ponemon-preparedness.html/.