NPC® Integrated Print & Digital Solutions
13710 Dunnings Hwy | P.O. Box 373 | Claysburg, PA 16625
P: 800.847.5757
F: 814.239.8706
www.npcweb.com

Data Breach Incident Response 0ÒÅÐÁÒÅÄ Î ÅÓÓ Self Assessment

When a Data Breach Happens, Are You Prepared to ...

- Mobilize your combined internal/external Incident Response Team to action?
- Contain and diagnose the problem leading to the breach?
- Employ a forensics team to determine the extent of the problem while evidence is still available?
- Make notifications in accordance with State and Federal laws?
- Provide continued Call Center support?
- Know with confidence that your forensic and notification providers will provide the data necessary to respond to Health & Human Services and Office of Civil Rights inquiries?

Are You Sure? The Following Self Assessment Will Help You Find Out!

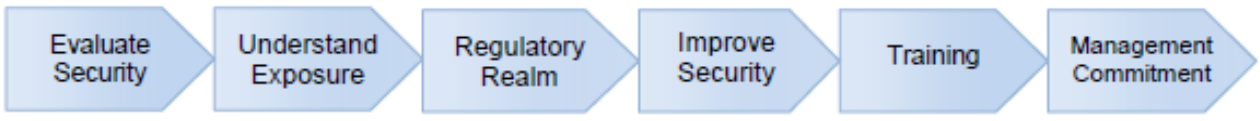
Insert the number of points after each question using the following point scores:

0 = No or Not Sure
1 = Somewhat or Partially Addressed
2 = Yes

Category A – Awareness and Preparation

Building awareness and preparation for a data breach is a mixture of having security measures in place and regularly audited, assessing your vulnerabilities, training and regularly updating everyone who touches personally identifiable information or protected health information in how to identify and report a possible breach at the earliest stage, understanding the regulatory environment in the event a data breach does occur, and direction and commitment toward data breach response preparedness from the Executive Management Team.

In a nutshell, awareness and preparation can be viewed like this:



The threshold for acceptable preparedness in this section is a minimum score of 15 out of 20 with no 0 scores. Results below this threshold require immediate action to reach a minimum level of preparedness.

0 = No or Not Sure
1 = Somewhat or Partially Addressed
2 = Yes

Results above this score still require commitment to continuous improvement of your incident response plan, your security measures, and regular refresher training for all personnel.

Have you laid the foundation to creation of an effective incident response plan?

1. Do you have a comprehensive IT Security procedure in place? _____
2. Do you have a comprehensive Physical Plant Security procedure in place? _____
3. Have you mapped the flow of private information through your systems? • _____
4. Do you have initial and follow-up security training programs in place? _____
5. Do your employees and contractors know how to identify a data breach? _____
6. Have you defined vulnerabilities and assessed risk of information theft or loss? _____
7. Are you aware of state by state and federal data breach regulatory obligations? _____
8. Are you aware of best practices in data breach response? _____
9. Have you assembled a data breach response team? _____
10. Is Executive Management committed to data breach response preparation? _____

Category A – Awareness and Preparation …… 0

Category B – Data Breach Response Team

Establishing and training the right team members, and getting buy-in from senior management, are critical in order to develop, maintain and implement an appropriate data breach response strategy. Due to the nature of a breach and the various state and federal requirements, it is often necessary to include representatives from Operations, IT, public relations, marketing, legal, customer service, privacy and risk (as well as others, depending on an organization's circumstances, as well as engagement of external service providers).

Each team member holds a key piece of information and a differing perspective relative to the development of an effective data breach response. Each team member may contribute in multiple ways, including impact assessment techniques, authoring the notification letter, coordinating media relations, or vendor management. Each link in the chain is critical. Knowing who is performing which response procedure is imperative should a breach occur.

The threshold for acceptable preparedness in this section is a minimum score of 15 out of 20 with no 0 scores. Results below this threshold require immediate action to reach a minimum level of preparedness. Results above this score still require commitment to the building and continuous training of your internal and external incident response team.

0 = No or Not Sure
1 = Somewhat or Partially Addressed
2 = Yes

Has your organization predetermined the team member(s) responsible for…

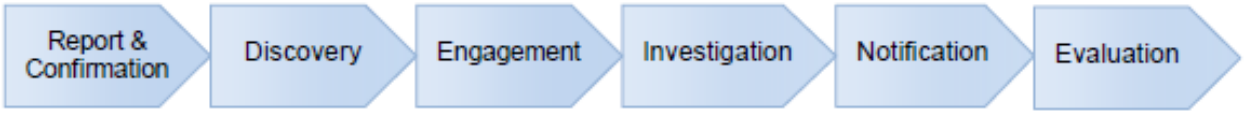
11. Coordination of breach response efforts? _____
12. Determination that a breach requiring notification of affected parties has occurred? _____
13. Determining the extent and scope of the breach? _____
14. Leading the breach response team? _____
15. Conducting the review of breach legal matters (e.g., criminal/HR issues)? _____
16. Development of content (and different versions) of notification letter(s)? _____
17. Signing the notification letter? _____
18. Primary contact with notification provider, forensic analyst and other 3rd parties? _____
19. Coordination of call center operations, including script? _____
20. Making the determination that a breach incident is closed? _____

Category B – Data Breach Response Team Score…… 0

Category C – Breach Management

Data breach response planning to effectively manage a breach event is now a business imperative, and Senior Executive Management must ensure adequate escalation, assessment, response and notification capabilities exist. The team must also be able to recognize, and management must be prepared to quickly authorize, the engagement of members of the external response team and any other professional expertise demanded by the situation.

In a breach response situation, an organization must answer numerous questions in order to effectively respond and manage the event. That is where preplanning comes into play and provides significant value. Having key questions answered upfront saves days and weeks worth of frenzied back and forth following a data breach. A typical data breach looks like this:



The threshold for acceptable preparedness in this section is a minimum score of 15 out of 20 with no 0 scores. Results below this threshold require immediate action to reach a minimum level of preparedness. Results above this score still require commitment to the refining and continuous improvement of your incident response plan.

0 = No or Not Sure
1 = Somewhat or Partially Addressed
2 = Yes

Has your organization established policies and procedures to follow for…

21. Escalation of a suspected breach situation to management? _____
22. Determination of the size and extent of the breach? _____
23. Determination of the nature of information breached (protected health or personally identifiable information)? _____
24. Determination of the cause of the breach? _____
25. Determination of when the breach started and ended? _____
26. Determination if a breach notification is legally mandated or warranted? _____
27. Determination of customers/employees impacted by the breach? _____
28. Determination of states of residency of the impacted individuals? _____
29. Determination of the third parties which must be notified (e.g., regulatory authorities; law enforcement)? _____
30. Notification of its insurance companies of the breach incident? _____

Category C – Breach Management Score…….. 0

Category D – Tactical Incident Response Plan

At a high level, it is important to carefully consider developing a tactical incident response plan including a plan assuring data breach notification capability. The plan must include breach management processes, workflows and protocols, as well as notice production and call handling capabilities. Formulating, in advance, approved tactical workflows and protocols will allow key tasks to be undertaken which follow approved guidelines.

An important aspect of an organization's breach response efforts is the ability to produce the legally-required notices and send them to the correct addresses of the customers impacted by the breach, whether by mail or email. In your planning, it is critical to establish a relationship with a vendor(s), capable of managing large scale breaches. They must have the capability and expertise to produce quality notification letters that preserve the organization's brand image and to manage all returned undeliverable notifications. Because of the high degree of connectivity between the mail/email notification and call center services, it is always ideal to select a notification vendor who can integrate both.

The threshold for acceptable preparedness in this section is a minimum score of 23 out of 30 with no 0 scores. Results below this threshold require immediate action to reach a minimum level of preparedness. Results above this score still require commitment to the refining and continuous improvement of your incident response plan.

0 = No or Not Sure
1 = Somewhat or Partially Addressed
2 = Yes

Has your organization established a tactical response plan outlining the process steps, workflows and protocols, as well as the vendor, to produce successful notification and FAQ response via call center support leading to Customer satisfaction and regulatory obligation fulfillment? Are you prepared to or have you ....

31. Obtained insurance to help mitigate the cost of the potential claim? _____
32. If insurance is involved, understood the requirements under the policy for vendor selection and coverage limits? _____
33. Vetted and are ready to engage a privacy attorney at the time an incident occurs? _____
34. Vetted and are ready to engage written notification, credit monitoring and call center providers that are dedicated to data breach? _____
35. Verified that the data breach response providers can operate within a tight compliance window whether the breach is 1 or several million? _____
36. Confirmed that your notification and call center data is readily available in an acceptable format in the event of a State Attorney General audit? _____
37. Confirmed that your notification vendor can perform Return Mail Management to handle undelivered notices, not just physically but also electronically? _____
38. Vetted a PR firm with data breach experience that can work closely with providers to optimize response and minimize brand damage? _____
39. Reviewed chain of custody procedures when notification occurs? _____
40. Determine the best method for data file transmission; e.g., encrypted email or secure FTP? _____
41. Created a draft of FAQ's to be used as a template for a breach event? _____
42. Engaged a notification vendor who can update the address list, identify deceased persons, and manipulate your address list to produce optimal mailing results? _____
43. Conducted internal training and communicated to staff in a manner consistent with the message in the FAQ's and media release? _____
44. Organized your tactical response plan into an executable workflow, together with assignments and responsibilities? _____
45. Demonstrated that you can execute the tactical response plan within the compliance deadlines required by applicable state and federal laws? _____

Category D – Tactical Incident Response Plan Score…….. 0

0 = No or Not Sure
1 = Somewhat or Partially Addressed
2 = Yes

Category E – Continuous Improvement

Your market and regulatory environment is constantly changing. You likely work hard to continuously improve service to your Customers. And consequently, your internal processes are changing. An essential element to an incident response plan that will fill your needs and grow with you is one that is continuously reviewed and improved.

If you achieve a score of at least 5 out of 10 and have the commitment to continuous improvement of your incident response plan, you are on your way. But you should not be satisfied if you are not showing convergence with 10 out of 10. By the very nature of continuous improvement, you would be lucky to achieve 10 out of 10 and would likely fall back if you did. But as long as you are asymptotically approaching 10 out of 10, you are doing great on this section!

Has your organization established a continuous improvement process that …

46. Updates IT and physical security procedures regularly, no less than annually? _____
47. Assembles the response team to simulate a data breach response at least annually? _____
48. Updates employee training programs and provides "refresh" training? _____
49. Provides at least annual analysis of vulnerabilities and risk assessment? _____
50. Evaluates CyberLiability insurance coverage at least annually? _____

Category E – Continuous Improvement Score…….. 0

SummÁÒÉÚÉÎÇ your results for Categories A through E, and subtracting 2 points for each zero score, youÒ overall ranking is:

Summary of Categories A through E …….. 0

- **60 or lower - Assign an executive team member to ÌÅÁÄ this ÉÎÉÔÉÁÔÉÖÅ!**
- **61 – 75 - Need work , ook for what is holding you back!**
- **76 – 90 - Very good, but need improvement!**
- **91 and Above - Fantastic!**

0 = No or Not Sure
1 = Somewhat or Partially Addressed
2 = Yes

Supplemental – HITECH Evaluation

The 2009 HITECH Act represents a significant expansion of HIPAA's requirements. They define the legal obligation to notify patients whose protected health information (PHI) has been breached. This notification obligation for HIPAA-covered entities also extends to data breaches caused by business associates with whom PHI has been shared. Breaches of PHI of 500 records or more must be publicly announced in the media and also posted on a Department of Health and Human Services (HHS) website. Harsh civil, and even criminal, penalties can be imposed by federal and state regulators for violation of these rules. As the use of electronic health records and health information exchanges increases, it is anticipated that breaches will continue to grow in both frequency and size.

The acceptable threshold for this section is a minimum score of 15 out of 20 with no 0 scores, with the exception of question A. Below this threshold, the organization must further review its capability to comply with the tough requirements of HITECH.

Is your organization aware of the following HITECH issues?

A. Does HITECH apply to your organization? If not, stop here. _____

B. Does your organization understand the differing responsibilities of a Covered Entity (CE) and a Business Associate (BA) when PHI is breached? _____

C. If your organization is a CE, do you have an up-to-date list of all your BAs? _____

D. Are there written Business Associate Agreements (updated for HITECH) signed with each BA? Have you updated them with each HIPAA/HITECH change? _____

E. Does your organization understand what personal information constitutes PHI? _____

F. What the relevance is of the "harm threshold" when PHI is breached? _____

G. What the time deadline is for a CE to notify patients that their PHI has been breached? _____

H. What information must be included in that notification? _____

I. How HHS is informed of a PHI breach? _____

J. Additional notification requirements if 10 or more notification letters are returned "undeliverable"? _____

Supplemental – HITECH Evaluation Score…….. 0