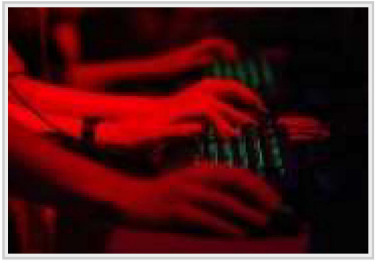
THOMSON REUTERS REGULATORY INTELLIGENCE COMMENTARY:
Six ways to maximize data breach plan effectiveness

Feb 12 2019 Steven H. Anderson



For firms that lack a plan for responding to data breaches, it is time to get one.

The latest data breach report (PDF) by the Identity Theft Resource Center (ITRC) tallied just over 1,000 data breaches in the United States, during 2018. U.S. data breaches hit an all-time high in 2017, with a total of 1,579 breaches, representing an increase of 44.7 percent over 2016. Research firm Cybersecurity Ventures has predicted cyber-crime damages will cost a staggering $6 trillion worldwide annually by 2021, a $3 trillion increase from their 2015 estimate.

The number of corporations experiencing data breaches has gradually increased since 2013, from 33 percent to 52 percent, according to data from the Ponemon Institute. Hackers do not discriminate. Breaches span companies of all sizes and across all industries.

Still, only 35 percent of companies have a fully realized data breach plan in place, according to cybersecurity publication CSO's 2017 U.S. State of Cybercrime survey. Other studies have reported up to 90 percent of companies lack an adequate response plan. This is an astonishing figure, given the cost that will be placed on companies who experience a data breach.

Even among those companies that do have data breach plans in place, their real-world responses are often disorganized. What good is having a data breach plan if it is not used for its intended purpose?

Here are six ways to get the most out of a data breach plan, by ensuring it remains actionable and relevant.

1. Ensure the plan is available

Some companies implement policies, but then let them die in a document, without making those policies

known. In addition to informing everyone in the company of the policy, it should be readily available for employees to access.

Host it on the cloud. This will help staff access the document in the event of an internal server crash. It is also recommended that you have a duplicate copy on a second host, just in case your cloud account is the one that is breached.

2. Keep it current

Your plan should be a living document. Hackers are constantly changing their methods to obtain data illegally. Just because you are prepared for an attack today, does not mean you will be prepared tomorrow.

It is important to revisit the plan regularly to ensure it responds to emerging threats and remains appropriate to the environment in which the firm operates. In addition to evolving hacker methodologies, other developments may affect the plan, such as legal and regulatory amendments or changes to corporate structure.

3. Consider your resources

A strong plan goes beyond listing the need to consult with an attorney and a company's business partners. Form a relationship ahead of time with an attorney specializing in data breaches, often called a "breach coach," and list out all your vendors and partners that will need to be contacted in the event of a breach. This should include your insurance broker, who can help initiate and navigate the insurance process.

Do not wait until after a breach happens to initiate these relationships.

4. Have a cheat sheet/checklist available

Chances are your plan is longer than a single page. When disaster strikes, do not expect your employees to go through each page of the policy to take proper action. It is recommended that you have a shorter version, or cheat sheet, to help them.

Checklists are great to have. Even pilots fill out checklists prior to take off. If they use one, so can your employees.

5. Practice the plan

If your first run-through of the plan occurs after a breach happens, then you are in for a big surprise. A breach will generate an enormous amount of stress for employees, and if they are not familiar with the plan, matters could get worse.

Rehearse the plan on a regular basis. Simulate events in real time to ensure all the right components are in place. Training employees to detect and defend against security threats is the best way to ensure your plan is implemented properly in the event of an attack.

6. Reach out to your insurance carrier

Keep in contact with your insurance carrier. The best carriers will offer you risk-mitigation advice to help your company protect itself from a breach. For those without a plan, your carrier will likely have information that will help you get started.

The average cost of a cyber attack is $5 million, according to Ponemon, which includes $1.25 million for system downtime. The statistics are staggering. We no longer discuss what to connect, but rather discuss that which is connected and how to protect it. A recent article by cybercrime expert Robert Herjavec, put it this way: "More connectivity. More points of vulnerability. More attacks. More risk."

Steven H. Anderson *is Vice President, Product Executive – Privacy & Network Security, QBE North America. QBE is an integrated specialist insurer operating in all key insurance markets, providing global capacity and expertise to meet customers' risk management needs shaped by unique exposures and changing business climates on local, national, and global levels.*