WHAT I'VE LEARNED FROM 5,000 DATA BREACHES

How has the breach response landscape changed over the last year?

Recently, the velocity and scale of breach events increased like never before. The Target data breach was a watershed event and marked the first time there was high-visibility executive turnover directly related to a breach. Now, consumers have raised their expectations and now expect a well-orchestrated breach response to begin the minute a breach is public. For businesses, this means the pressure to get it right the first time is more intense than ever.

After a breach, losing customer trust is a big concern for brands. What can companies do before and after a breach to ensure customer trust remains intact?

Companies should place excellent customer service at the center of response planning and execution. Taking the time to plan for an incident with the customer in mind will go a long way in preserving customer trust when a breach occurs. All communications to customers need to be clear and helpful to minimize confusion and anger, and it is much easier have clear communications when you think through the flow and complexities in advance of a real incident. Keep in mind, your customers' first interaction with your brand after a breach may be with the call center, so getting that experience right is crucial to success. A responsive and knowledgeable call center using agents who are trained in identity theft protection reduces customer anxiety and angry escalations. We have also found that customers aren't comfortable giving up their personal information to enroll in protection services after feeling violated by a breach. You should look for solutions like the program we offer at AllClear ID that offers automatic access to identity repair to create the best experience for affected customers.

What is the single most important thing companies can do to ensure a breach response goes smoothly?

In my experience, companies across all industries that focus on their customers before, during, and after a data breach fare far better than those that do not, both in terms of overall response and the speed at which they are able to return to normal business operations. Many modern businesses have a special relationship with customers as often there is high frequency of interaction and strong brand loyalty. To successfully manage a breach with a customer focus, companies must first have a plan in place. This will help save significantly by avoiding delays and costly mistakes during the response. Now that we have witnessed the first destructive cyberattack against a US company, having an incident response plan in place is no longer optional. These plans should include details for how affected customers will be notified and supported throughout the entire response process, from notification, to protection, to fraud resolution, if necessary.

Many of the largest breaches in recent years occurred in the retail sector. How is responding to a retail breach unique compared to incidents in other industries?

Retail point of sale breaches present unique challenges that warrant a particular type of response effort. In many cases, tens, if not hundreds, of store locations or franchises are affected, making consistent dissemination of information and communication challenging. Further, retailers do not always have direct contact information for those affected by the incident so it is not always possible to isolate and contact specific individuals affected. Complicating these matters is the fact that the press frequently reports these types of incidents before the company, so the response timeline is compressed and out of the retailers' hands from the start of the incident. While each breach is unique, these dynamics make proper preparation particularly important when responding to retail breaches.

Jamie May is Vice President of Operations at AllClear ID. Since joining the company in 2007, she has managed the implementation and execution of over 1000 data breaches, including some of the largest healthcare breaches since the creation of HITECH, and one of the largest retail breaches in history. She advises Fortune 1000 companies, government agencies, and healthcare organizations on all aspects of breach preparation and response and is a sought-after industry expert.

Contact us to learn more: www.AllClearID.com/business

Benefits of Working with AllClear ID

Customer Focus

The key to an effective response is happy customers.

Expert Advice

Work with the most experienced team in customer security and breach response.

Confidence

Meet high expectations of customers, shareholders, and the media.