SonMax Consultants Inc.
24 Manor Drive
Marlboro, NJ 07746
E: sales@sonmax.com
T: +1 732.591.1512
F: +1 732.591.5424
www.sonmax.com

The Tale of Two Breaches or How Not to React to an Incident

Over the last few weeks, several very public breaches have reached the news. One, composed of least 143,000,000 personally identifiable information (PII) and personal card information (PCI) records, is the result of Equifax's breach starting in March of 2017. The second, consisting of millions of credit and debit card accounts, is due to the breach of Sonic's store payment systems.

The differences in both the breaches themselves, and the response of the two firms, provides a stark example of how to and how not to respond to an incident:

1. Equifax's breach occurred in March but was not discovered until the May/June timeframe. Despite that, Equifax neglected to inform the public until September 2017. Equifax did employ a reputable 3rd party forensic firm – but not until the latter part of June and did not provide good data to the forensic firm – resulting in delays in getting good scope around the breach.
    a. Equifax additionally tarnished their reputation by acknowledging, after the fact, that a number of executives had sold blocks of stock in Equifax. These sales happened after the breach, but before the public release of the breach
    b. Equifax's CIO and CISO suddenly "retired"
    c. Equifax's CEO suddenly "retired"
    d. Equifax changed the terms and conditions of the credit monitoring offering, after many customers complained about the Equifax requirement to be shielded from legal liability

SONMAX
CONSULTANTS INC.

    e. Equifax subsequently had a problem with their twitter account being compromised, and a tweet contained a URL that sent followers to a bogus credit processing site – potentially another hack of the Equifax brand

2. Sonic's breach occurred in the August/September timeframe – while the exact timing is not yet clear, the first evidence of a compromise was reported on September 18, 2017, when some five million credit card and debit card accounts were put up for sale in ***Joker's Stash***, a well-known, dark web, credit card theft bazaar. Sonic readily admitted that there had been "a potential incident" and advised that a 3rd-party forensic firm has been engaged and that law-enforcement (read, FBI, among others) is actively working the case.
    a. While Sonic does not yet know how many of its 3,600 locations, in 45 states, were impacted, it does know that at least 5,000,000 cards were compromised.

There are several glaring issues that immediately come to light here:

1. Sonic discovered the breach in a matter of weeks, as they got a report from their 3rd party credit card processor. They immediately engaged a 3rd party forensic team and have gotten out ahead of the bad news. All in about a month. Any damage, from Joker's Stash, started on or about September 18, only 11 days ago.
2. Equifax did not engage a 3rd party forensic team for almost 3 months. They did not reveal the breach for almost 3 **additional** months. In opening a portal to consumers who wanted to get information, they provided misleading and sometimes false information to consumers. Their executive team did a poor job in communicating issues to the 3rd party forensic team and to the public. And the numbers associated with the breach keep growing. It is not yet clear that the 134,000,000 number will be the final number.
3. Sonic sells food
4. Equifax sells personal and credit data on hundreds of millions of people. Additionally, Equifax made a strong public case that their security around the personal and credit data was not only supreme, but a primary business driver in the market
5. Sonic has been fast, open and transparent in their message to the street
6. Equifax has been slow, opaque and inconsistent in their message to the street

Whom do you think executed the incident response plan correctly? I suspect you figured out the answer.

It's all about the Incident Response Plan and executive leadership.

Please follow me on twitter: @stevewertheim