The Data Protection Series: #1 What happens in a Breach?

"*There are two types of companies: those that have been hacked, and those who don't know they have been hacked*."-John Chambers, former CEO of Cisco. Mr. Chambers probably didn't know how correct he was when he made that statement years ago. Nowadays a breach of any data system can lead to massive regulatory obligations.

It's well accepted that there is no perfect security system in the world as is regularly shown to us by hackers. A few recent examples include NotPetye and WannaCry. It is not a matter of if your system will be comprised, but when. Isn't it better to have the contingency set in place beforehand? Apart from ensuring that a company can continue running with as little disruption to its customers as possible, there may also be government agencies that must be informed of the breach. Some countries impose massive fines if the government isn't informed, especially in cases of healthcare or financial information being inappropriately accessed.

Following the breach and access to potentially 143 million customer's personal information in the U.S. based credit monitoring giant, Equifax seemed to have a decent contingency plan, but as the weeks since the breach was publicly announced on September 7 passed, it has become clear that their contingency plan wasn't remotely as strong as it should have been.

Forty-eight states in the U.S. have legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information. Each state has different requirements based on the timeframe, what kind of information is covered, who must comply with reporting requirements, but the overall trend is the same. Giving notice of a breach to affected persons is required. The public wasn't informed of the breach for at months after the March hack occurred. Information accessed by the hackers included the names, addresses, Social Security numbers, dates of birth, potentially driver license numbers and more of roughly 40% of the American population, information that can make it incredibly easy to steal a digital or financial identity.

Equifax seems to be a perfect example of what not to do.

The public relations nightmare Equifax is dealing with in the fallout of the breach serves as the first reminder as to why companies need strong and regularly updated contingency plans in case of breach. Regulatory agencies like the Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission are going to be beefing up its oversight of companies with access to such sensitive information and have already indicated that preventive credit monitoring will become a standard. The New York Department of Financial Services (DFS), which issued a subpoena to Equifax demanding more information about the breach. Other states are expected to investigate or directly sue, like California, as well. Equifax is dealing

Samantha Bradshaw, Eptalex ATLF Beirut
All rights reserved- 2017

with federal laws, federal regulators, state laws, and state regulators in a dizzying patchwork of data protection laws.

Federal laws give the CFPB the power to supervise and examine large credit-reporting firms to ensure the quality of information they provide. In January 2017, the CFPB fined TransUnion and Equifax $5.5 million for deceiving customers about the usefulness and cost of their credit scores. More fines can certainly be expected for Equifax in addition to being the watershed moment for a whole new gamut of regulations over consumer financial data.

While most companies don't sit on the proverbial 'gold mine' of personally identifying information, they still collect it to some extent and store similar information. Equifax is facing such a complex situation because they operate in literally every state in the US, so every state and federal regulation that covers data protection, consumer protection and financial information is coming into play. However, that's exactly what companies, even outside of the US need to understand; storing data isn't simple anymore and dealing with a breach is even more complicated.

California state law, albeit one of the more advanced states in regards to data protection requires that data holders provide a notice of a data breach to the regulatory agency with 72 hours of learning of it and to affected Californians without undue delay. Equifax's contingency plan, or lack thereof, doesn't appear to comply with that as the public announcement occurred many weeks after learning of the breach on July 29th according to Equifax. The credit monitoring company is now being sued for violating this law in San Francisco. The natural fix for having to navigate 48 states laws is a federal law, but pushes to create a federal data protection system could preempt stronger state data protection laws like those in California.

At the federal level in the US, the data security laws that exist are typically industry based. We see a perfect example of this is the massive regulatory scheme applicable to banks, yet for credit reporting agencies, the scheme is relatively lax. In Europe, the EU has laid out some basic principles for general data protection in recent years, but follows the same route as the US in having more detailed and rigorous regulations in certain sectors like banking and healthcare.

With small, medium or multinational company operating in an interconnected world, chances are that each company winds up collecting personally identifiable information and chances are they will be the target of a hacker at some point. The logical step is to prepare for the inevitable breach. Initial steps are all preventative and ensuring that the system is as segmented and protected as reasonably possible. Companies should look to IT professionals for options on how to isolate and mitigate the threat of a breach. However, once the breach happens, none of the preventative things matter as long as they met the minimum standards for each country that can claim jurisdiction over the information on the hacked server.

The compliance requirements that should be built into a reaction plan need to be comprehensive of all the potential information on the hacked system. In healthcare, finance

Samantha Bradshaw, Eptalex ATLF Beirut
All rights reserved- 2017

and generally sensitive data, there are typically specific regulatory agencies in the more developed jurisdictions.

In the EU, Regulation 611/2013 states that fines for non-compliance with post breach obligations can go up to 2% of the total worldwide annual turnover. However, a new e-Privacy Regulation will enter into force on 25 May 2018, the same date as the General Data Protection Regulation (GDPR) (Regulation EU 2016/679). This appears intentional to show the harmonious relationship between the two Regulations. The new law will keep a similar breach notification requirement as currently exists for EU Member States. However, certain sectors have additional requirements they need to look to as the law develops in the EU.

Samantha Bradshaw, Eptalex ATLF Beirut
All rights reserved- 2017