What Can Reinsurers Learn from the Equifax Breach?

DARREN WRAY

What Can Reinsurers Learn from the Equifax Breach?

Despite the first attacks on Equifax going back as far as May 2017, the full details of the breach have not and may never be fully released to the public. There is, however, enough information available for those on the outside of the organisation to observe the lessons that can and should be learnt.

Before we get into the details, it is important to understand that although Equifax made mistakes, they're not the only company to do so. Their biggest mistake, however, was in not having a means of recognising the mistakes that had been made and mitigating the situation before it became the issue it is today.

What Makes the Equifax Different

Understanding and knowing what is different about Equifax helps in appreciating the value of the lessons that it has to teach us, so here are some high-level facts.

Number of People Impacted

The Equifax breach is one of the largest data breaches or all time, with over 160m people's personal information (name, social security number, address, contact information, driving licence information, etc.) being compromised. While there have been previous breaches, the level of personal information that was taken during this breach makes it one of the most potentially damaging incidents.

The Timeline

According to the post-breach analysis, Equifax was initially hacked in March: according to some sources, they did notify some parties external to the organisation but it was kept pretty quiet. The main data breach occurred in May and June. It is believed that the majority of the data was taken during that period. The first report of the notification of the issue was made on September 18th, meaning that the data that was taken in the first part of the May-June attack had been "in the wild" for at least four months.

Share Trading

In early August, almost 3 months since the start of the main breach and a month before the public would be made aware of the incident, three senior executives (the CFO, president of U.S. Information Solutions and the president of Equifax's Workforce Solutions business) sold more than $1.75m of shares in Equifax. Equifax has stated that there was no impropriety and that these people were unaware of the data breach. A congressional commission has been formed to investigate if insider trading laws were violated.

Right People for the Role

There has been much made of the fact that both the Chief Information Officer (CIO) and the Chief Security Officer (CSO) were not the right people for the role. It has been said that the CSO did not have the technical background expected of someone in this role. I do think that these are important details. Some of the vitriol on the Internet following the discovery of this news, however, may not have been proportionate. The suitability of staff is ultimately the role of their organisation. There is not enough information in the public domain to determine in this case but if Equifax had put itself through an external cybersecurity assessment some of the shortcomings would have been identified.

+44 (0)20 7193 1966 enquiries@fifthstep.com www.fifthstep.com

Lessons

The lessons for reinsurers can be divided into two types: the lessons that they need to learn and apply to internal and vendor provided functions, and those needed to ensure that the ultimate policyholders are learning.

Lesson 1 – Have and Use an Incident Response Plan

It is difficult to tell how much of an incident response plan Equifax actually had. Going on the evidence alone I would say that it certainly did not live up to the expectations that I would have for my clients, for the primary reasons that while Equifax hired cybersecurity specialists to deal with the May-June breach, the actions taken after the March incident seem to be wholly inadequate, with the incident being largely ignored.

The May-June event was discovered in July, but those whose data has been compromised were not informed until September. A data breach plan should include the following as an absolute minimum:

Stop the Breach/Attack

The first step is to stop more data being stolen. Inherent in this is a technical understanding and an initial triage of the attack.

Communications Plan

A good data breach response plan will identify the stakeholders for the organisation. Some will be internal (The Board and senior management), some will be trusted third parties (non-exec directors, third parties assisting with the breach, law enforcement if/where required). Others will be customers (those effected by the data breach for example) and for those in regulated sectors or that are subject to data protection legislation by the regulators.

As a minimum, the communications plan should identify the frequency (hourly, daily, weekly etc.), type (email, social media, press, TV etc.) and level of detail of the communication to be provided. The plan is likely to be adjusted with the severity of the breach with guidance on how this should be achieved and included as part of the communications plan.

Initiate the Business Continuity and Disaster Recovery Plan

An incident response plan has many purposes, but a key one is to initiate the recovery process. This may be based on the initial information and triage but it is imperative to protect the organisation, its people, its assets (digital and physical), and its reputation.

The reinsurance sector is highly regulated. An incident response plan is becoming a mandated required requirement. The NY DFS cybersecurity requirements in the US (NYCRR500), for example, demand this. The requirement is also part of the European data protection (GDPR) and breach reporting requirements that come into place in May 2018.

Lesson 2 – Communicate with Regulators and Data Subjects

The second lesson learnt from Equifax goes back to their communication plan, or seeming lack of one. The news broke and as a casual observer, there seemed to be very little information or PR control.

Data subjects were largely left to contact Equifax for information, which overloaded Equifax's ability to answer the calls. Their website had stock information that left many people wondering what they should do and whether their information was involved or compromised.

It is also important to mention that this confusion came several months after Equifax had discovered the breach. Even if they only had an outline plan before the breach they don't seem to have made good use of the time from point of discovery to point of announcement.

72 hours is considered to be the right amount of time from discovery to the first announcement, this is included in data protection and cybersecurity regulations around the world, including NYCRR500 and the GDPR.

+44 (0)20 7193 1966 enquiries@fifthstep.com www.fifthstep.com

Lesson 3 – Be Prepared

I don't think it is unfair to say that Equifax was surprised by the attack, but given the time between discovery and the public announcement, it is evident that they really were not prepared.

One example of this is the system that they provided to check if details had been compromised (a good idea in its intentions), this required more personal information than was ideal to be passed to another site, which is concerning. The website itself had a domain name that looked suspicious (www.equifaxsecurity2017.com), and the domain name was registered shortly before being deployed which also made it look suspicious to the more technically aware.

I'm sure there must be a good reason why they didn't use something like www.equifax.com/security but all of this points to an organisation that was unprepared and is having to react to a situation rather than following and adapting an incident response plan.

Lesson 4 – Privacy and Security by Design

The system that caused the challenges for Equifax was not a major system at the heart of their network, it was offering a simple service. The trouble is that while the web server software deployed by Equifax didn't need or use all of Equifax's assets, it was trusted by those assets and when it was hacked, it was able to access information that it had no business accessing.

This is at the heart of privacy and security by design, which can be summarised as designing systems and permissions to have the minimum access required to do their job. This means that should that system be compromised either by a hacker or perhaps an unexpected bug that the system isn't a portal to the rest of the enterprise.

Lesson 5 – Patch, Patch and Patch Some More

While information about the cause of the data breach are not fully public and may never be made so, what has been released suggests that the web server that was compromised had software on it that had not been updated (or patched). The software vendor had released a fix to a critical security vulnerability in March and this still hadn't been applied by May when it was fully exploited.

IT teams need to ensure that patches are applied promptly. Once a security patch has been released by a vendor, the details of the issues that it is fixing are very often reverse engineered by bad actors so that they can search for machines that have not yet been updated.

The Consequences

The reputational damage to Equifax and the credit checking industry as a whole has certainly suffered. This includes organisations whose only connection to Equifax is that they work in the same sector.

High-ranking members of staff have left the organisation since the data breach, including the CIO and CSO, and the House Energy and Commerce Committee has questioned the CEO of Equifax.

On the direct financial side. Equifax's shares dropped 13% in early trading the day after the breach was made public and are down by over 25% since the announcement in September. As I write this article, a number of law suits have been filed (a class action by Canadian consumers was seeking damages of 450Bn USD, another US based class action is seeking 70Bn USD), so the financial cost of this breach is likely to be difficult to calculate for a number of years.

How would I summarise the lessons that your organisation should learn from the Equifax breach? You must be prepared and able to react, respond and recover promptly, while reassuring your customers, investors or other stakeholders that you have the situation under control and are fully prepared for all eventualities.

Darren Wray is an author of books on Data Privacy and IT Leadership and is the CEO of Fifth Step, a company that helps insurers and reinsurers to improve their resilience in the face of the cybersecurity risks that they face. You can find Darren on LinkedIn and find out more about Fifth Step at www.fifthstep.com.

If you need help with changing your organisation's ability to become compliance then please speak with Fifth Step. You can find outmore about us and our current thinking at www.fifthstep.com or by following us on with either Twitter @FifthStep and on LinkedIn.

+44 (0)20 7193 1966 enquiries@fifthstep.com www.fifthstep.com