In 2015, Anthem, the second largest US health insurer, had been subject to a cyber attack. Data of 80 million clients and Anthem staff respectively had been affected. The data stolen entailed names, domestic addresses, date of birth, email addresses, employers contact details and Anthem staff salaries. It is highly likely these data found their way into the dark web and were sold for criminal use.

Although the data loss had been massive and the case severe, the Anthem crisis management for the most part proved to be highly professional.

Quick response and transparent communications

Luckily, neither the media nor the authorities detected the breach, which put Anthem into a more comfortable position for the crisis response and regaining trust. The technical warning systems and internal response protocols worked well. Although Anthem was legally obliged to inform the affected individuals and organizations of the data breach within 60 days, the company decided to inform all stakeholders including the public domain already after eight days. This prompt response helped to regain trust and demonstrate transparency. Anthem in detail declared what data had been compromised, which data had not been affected and what Anthem would do next.

A delayed communication or no communication at all will always be detrimental, as other stakeholders will sooner or later start communicating anyway and thereby set the narrative and frame.

Crisis response and containment

Anthem notified the authorities and supported the investigations rigorously. Furthermore, the insurer offered support to the individuals affected. A specific website was implemented that contained FAQs and a hotline with specifically trained staff replied to individual questions of clients. Clients responded positively to the effort of the insurer as they could easily manage to obtain the information they required and have individual queries responded to in due time. As part of the Anthem support the company tasked an IT security provider to monitor the credit cards of individuals affected for the upcoming 24 months and offered these services free of charge to all individuals affected.

In cases like this, individuals affected always expect straightforward answers to the potential impact on themselves, what they should do, in what way the organization subject to the breach may support and what further prevention measures will be implemented.

Taking responsibility

The Anthem CEO publicly responded to the incident in a letter. He apoligized to clients and employees and showed sympathy for their irritation and annoyance. He made it clear that his personal data had been breached too. Legal advisors mostly are hesitant or reluctant when it comes to apologies in public as they may be misinterpreted as an admission of guilt. However, from a crisis management and crisis communications standpoint, a formal apology in due time will be crucial, though it has to be drafted carefully.

Risk prevention

Anthem did well when it came to a decisive crisis response, though the underlying risk prevention proved to be poor. The data compromised had not been encrypted. This is surprising as a number of cyber attacks in the past suggested that potential victims of cyber attacks were highly likely to protect the data more diligently. Even a high level of IT-security will most likely not prevent perpetrators from infiltrating the IT-infrastructure one way or another. However it should be possible to create numerous rings of defense and effective early warning systems.

Effective preparedness always should entail straightforward emergency and crisis management structures, effective internal response protocols and 24/7 access to professional emergency, forensic and crisis response consultants. A number of insurance solutions provide the resources required.

SmartRiskSolutions GmbH

SmartRiskSolutions is specialized in security consulting, crisis management, and travel risk management. With our team of experienced consultants, analysts, instructors and international partners we support you wherever hazards put your business, organization or staff at risk. As we on a regular basis are conducting crisis response consultancy to insured clients facing extortion, kidnap for ransom, malicious product tampering, cyber attacks or other threat events we know what kind of emergency and crisis management structures work effectively and which do not.

by Pascal Michel
and Marc Brandner, SmartRiskSolutions GmbH