STORM Guidance

Strategic, Tactical & Operational Risk Management

Assess | Plan | Respond

Comment on Guidelines 01/2021 on Examples regarding Data Breach Notification

Date: **24th January 2021**

Document Owner: **Neil Hare-Brown**

Guidelines 01/2021 on Examples regarding Data Breach Notification

This document is an excellent first step to ensuring organisations are clear on their responsibilities for the effective management of data breaches.

I am the CEO of STORM Guidance and have over 30 years first-hand experience managing a range of cyber incidents. My book, Information Security Incident Management: A Methodology, is well read by first responders around the world.

At STORM Guidance we have responded to hundreds of data breaches in the last six years. Our work is mainly focused on cyber incident response for leading insurers. We are the founders of the ReSecure service (www.resecure.global) and respond to cyber insurance claims and have had the opportunity to work on cyber incidents and breaches in large and SMB organisations located in UK, EU, US and Canada and operating across many different sectors. ReSecure provide digital investigations, legal, crisis PR and surge notification services as a single point of expertise for insured organisations.

On reading the consultation guidelines I found that the breach scenarios described are somewhat inconsistent with the current trends in cybercrime and data breaches. One important type of incident, currently the second most prevalent type of incident, is Business Email Compromise (BEC) new incidents of which we respond to on an almost daily basis. BEC incidents are often significant data breaches because target mailbox data is often extracted as part of the attack. An example is that attackers in possession of stolen mailbox credentials, will then synchronise the mail with a new rogue client (often a mobile device) so that they can prepare and execute financial fraud on the owner of the mailbox or a third party.

BEC attacks often require rapid and accurate identification of data subjects at risk of fraud, identity theft and reputational harm. Our team have developed a comprehensive process called Mailbox Content Analysis (MCA) consisting of both automated (using machine learning) and manual (using a team of analysts) to identify PII, then classify it and finally analyse it to find data subjects at high risk who can then be notified. Few cyber investigation teams do this, but we consider that it is necessary to prevent cybercriminals leveraging breached data to cause further harm to data subjects.

I would recommend you consider including BEC incidents in your scenarios and would be pleased to assist in anyway needed to ensure this paper is of real benefit to the fight against cybercrime and the protection of data subjects at risk.