COSMOS
Navigate the Compliance Universe

CEP Magazine - July 2020
Two years of GDPR: The security breach lessons we've learned

By Jonathan Armstrong

Jonathan Armstrong (jonathan.armstrong@corderycompliance.com) is Partner at London-based Cordery.

- +44 (0)20 7075 1784

Dealing with a security breach, even in these unusual times, is the toughest aspect of a compliance professional's job. Since we've passed the second anniversary of the General Data Protection Regulation[1] (GDPR), I thought it might be interesting to share some of the lessons—the top ten tips—that my organization has learned from handling security breaches across the European Union. We have also included some public cases from around the EU and further afield to illustrate some of the points we are making. In some cases, we have used pre-GDPR cases where we think they are instructive. Most of these lessons seem like common sense, but it will be to your advantage to review them as a checklist to make sure your processes are robust.

Tip #1: Have a plan

It is a simple fact of life that data breaches are inevitable, and for most organizations, even the best ones, it is a when, not an if. Once you're in this mindset, it is easier to understand that you have got to prepare. A lot of the issues we see are where clients either do not have a plan or have a plan that is so detailed that nobody refers to it when there is a breach. A really technical 45-page plan that you ask employees to read is as good as having no plan at all. What most organizations actually need are two plans:

1. A simple plan for employees to follow that tells them how to recognize a breach and what to do when they see one. We often liken this to the type of notice that you get on the back of a hotel door telling you how to raise the alarm and get out of the building. Try and keep it just as simple, with clear guidance. There is another parallel with these fire safety signs: we used to also tell people which fire extinguisher to use for which type of fire (i.e., data breaches) and how to work out the source of the fire. We do not do that anymore. Now we just tell people to raise the alarm. One of the real causes for a delayed response is that people sometimes think they have to report a problem *and* a solution. They don't! Your obligation is to report a problem, and in most cases, it will be down to the team of experts to work out a solution (or at least mitigation). This might be where the second plan comes in.

2. A more detailed plan that the data breach team uses as their guide. This team also needs to rehearse. We have had real success with our "Data Breach Academies," which walk data breach teams through a realistic scenario. It works a little bit like muscle memory. Once the team members know each other and how they worked together in the simulation, they will work better together and respond more quickly to reports.

Tip #2: Know your data and third parties

There are a lot of issues around data in modern-day organizations, partly because they outsource tasks that even five years ago would have been regarded as a core function, so many organizations do not know exactly where their data are. We have been involved in breaches where a third party has told the compliance team about a data breach, and the compliance team did not even know that the vendor was being used. Organizations must do

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

proper due diligence on providers and have proper contracts in place.

This goes for acquisitions, as well. The Marriott case[2] illustrates the need to do proper due diligence during the acquisition of an organization to make sure there isn't a hidden issue. For many organizations, this will be a board-level responsibility; for example, see the words of Information Commissioner Elizabeth Denham in the Equifax breach:

"'*Multinational data companies like Equifax must understand what personal data they hold and take robust steps to protect it. Their boards need to ensure that internal controls and systems work effectively to meet legal requirements and customers' expectations.*'"[3]

This document is only available to members. Please log in or become a member.

Become a Member Login

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.