

# Third Party Data Breaches

## Out of Sight – Out of Business!!



### The newsworthy and the not so newsworthy

At the time of writing, Sony have just confessed to suffering two hacking incidents in the space of a single week which together affect well in excess of 100,000,000 PlayStation network accounts. Customer identities, as well as their bank and credit card data, have been compromised on a grand scale. Indeed, it feels that not a week goes by without there having been at least one notable headline advising us of how a well known organisation has suffered a serious data security breach. We all know that it won't

hit the front pages unless it involves a large corporation or high profile government agency but what about all the other, not so newsworthy data breaches that thousands of organisations encounter each year?

Serious data breaches should be reported to the Information Commissioner's Office (ICO) and indeed the ICO is warning that all organisations may face tougher sanctions if they fail to report breaches which subsequently come to light. Some of these will be newsworthy but the majority will not. We should also bear in mind that these reported examples are the ones that have

actually discovered a breach; but how many others out there have yet to discover that their doors are wide open to a potential incident?

### Should we share our data?

While drastic measures like pulling the plug on your internet connectivity are probably somewhat extreme, the reality is that data is only of any use if it can be used and, increasingly nowadays, shared.

The majority of us are familiar with the issues surrounding the sharing of data but how many of us really understand or have the appropriate controls in place to reduce or prevent an actual breach?

### Where are the boundaries?

Whilst organisations are getting better at managing their data risks, once this data has been shared with a third party it appears that we have significantly less control (if any) over it. There is also a misplaced belief that the failsafe of a

contract will remove you of all your liabilities. Whilst a legal obligation may well reside with the third party, the Data Protection Act 1998 clearly states that the organisation from where the data originated is classed as the “Data Controller” and as such remains accountable for that data throughout its lifecycle. As such, the data and the associated penalties – whether they are financial or reputational – still very much reside at the point of origin.

Unfortunately, in many instances, it takes a data breach or a near miss before the boundaries are clear to all parties.

The recent email breach at marketing firm Epsilon is an example of third party data breaches. Epsilon's database was hacked, exposing the email addresses and names of people with whom Epsilon's clients do business. Epsilon's clients include both professional services and corporates.

### **The List of Unknowns**

We have assisted many organisations with managing their data risks, particularly in respect of third parties. This has highlighted some particular issues, which we refer to as the list of unknowns.

**Unknown: How many third parties have access to your data?**

You may be surprised to learn that most do not know how many of their third parties have access to their data. They tend to be able to list their third parties whether via an Approved Supplier or Preferred Supplier list or database; however, ask them if they understand what data is being shared, with whom it is subsequently being shared, for what reason and with what controls, and the response is all too often one of uncertainty.

**Know ALL of your third parties. Risk assess them and if necessary audit them!**

**Unknown: What is in the contract? (Or in some cases, where is the contract?)**

In many cases, a well written contract agreed by both parties should suffice. Both parties should have a clear understanding as to their respective expectations through established service levels, security schedules, independent review and ongoing relationship management. It's when things don't go as planned that the contract is invariably referred to, and it usually comes as a shock to one or both parties that on closer inspection there is, for example, no “right of audit” clause, enforceable service level agreement, or clause stipulating that the third party is required to adhere to your Information Security policy. It's an even bigger shock when you can't

locate the contract. These are typically contracts with smaller third parties, either one-offs or third parties with whom you have an established relationship.

Nonetheless, they may still have access to your data and you are still legally responsible for its well being.

**Have a contract with each and every supplier, know what's in it and know where it is!**

**Unknown: What data does each of your third parties have access to? And do they need access to all that data?**

Many third parties require access to your data; unfortunately many organisations are leaving the decisions regarding to what data they should and shouldn't have access far too late in the process. After all, the third party knows best – they are the experts, aren't they?

Only allow third parties access to your data on a strictly need-to-know basis. What is of particular concern is when they do not know what data their third parties can access.

**You need to understand what access your third parties have and what they are accessing!**

**Unknown: What do your third parties do with your data? And more importantly, what do they NOT do with your data?**

Once that data is out of your door, it's out of your hands and

in the hands of your third party. Many organisations seem to be closing their eyes and hoping for the best. Some simply rely on an Information Security Policy which the third party flashes about telling them all the wonderful controls they have in place to ensure the customer data is secure. In reality, this is just a document and worthless if it isn't acted on and effectively implemented. You should know exactly what third parties do with your data; from how it's stored, processed, protected and with whom it's shared and so on, to whether the third party is actively working to continuously improve their controls. Increasingly, organisations are actively assessing their third parties' technical capabilities and also procedural activities in relation to Information Security.

**Understand exactly what your third parties do and don't do with your data!**

*Unknown: What has happened to your data after the relationship with your third party has ended?*

Winding down a relationship with a third party can take a considerable amount of time and effort. Most organisations are relatively proficient when tidying up financials, ensuring that skills and knowledge are retained and transferred, but very little is being done to ensure that ALL of the data is removed or disposed of securely. Imagine getting a call from a third party years after terminating a contact with them advising you that the data belonging to you they didn't know they still had, had been compromised.

**Ensure that ALL data that you shared with the supplier is either returned or permanently deleted from their systems.**

**Turn your unknowns to your knowns and manage your risks**

Most organisations tend to think that the worst will never happen and that the controls they apply in respect of their data are sufficiently robust. The reality, as has been well reported, is often very different. Invariably it's easier and more cost effective to prevent a breach from happening rather than deal with the consequences.

**Kingston Smith Consulting LLP, the business protection consultancy, has the experience that you need to make your unknowns known.**

---

### **About Kingston Smith Consulting LLP**

Kingston Smith Consulting is the specialist consulting practice of the top 20 accountancy firm Kingston Smith LLP.

Kingston Smith was originally formed in 1923 and the firm has grown to its current position through organic growth and mergers. Kingston Smith is a member of KS International which is an association of independent accounting firms in 50 countries around the world.

#### **Kingston Smith Consulting LLP**

Devonshire House, 60 Goswell Road, London EC1M 7AD, UK Telephone +44 (0)20 7566 4000 Fax +44 (0)20 7566 4010  
[info@kscllp.co.uk](mailto:info@kscllp.co.uk) [www.kscllp.co.uk](http://www.kscllp.co.uk)

A list of partners is available for inspection at the above address.

Registered in England and Wales as a Limited Liability Partnership: No OC341786 Registered office: Devonshire House, 60 Goswell Road, London EC1M 7AD