How to Manage a Company Cyber Breach

We have often seen in the press that those companies who have experienced a cyber breach and were not prepared have suffered significant brand damage. In some unfortunate circumstances this has even translated into high levels of customer churn. Whilst you can now buy an extension to your cyber policy to cover loss of revenue linked to a cyber breach it would obviously be better to avoid the damage to your brand in the first instance.

Being prepared to tackle this crisis situation, and having an Incidence Response Plan detailing who to contact internally and externally during the process can result in a smoother response, limiting reputational harm. We spoke to Adrian Phillips to ask him for his thoughts and experience on how best to manage a cyber breach.

Tell us about your background and your current role

After a number of years practising at a large city law firm, I started my in-house career as General Counsel and Head of Risk and Legal Affairs for Visa in the UK. I then moved to San Francisco where I became the Deputy Chief Risk Officer for Visa globally. My next role was Head of Legal and Privacy at Amadeus in Madrid. Now I am General Counsel at 441 Trust Company Limited as well as Special Counsel at Jones Day. I believe that my various roles have given me an interesting insight into the myriad of issues associated with data breaches.

What happens when there has been a data breach?

It rarely happens that someone says: ‘we’ve been hacked’. You start seeing strange things going on in subsidiaries or in your own company. Someone notices something unusual from a technology perspective, for example in the software, looking at the data leaving your system. It could also be that someone loses their computer or a disk. Keep an open mind as to whether it is an internal or external culprit—over half of breaches are by insiders.

Being contacted by the police or your bank is another indication. With cardholder information, what normally happens is that cardholders will call their bank to say they have noticed unusual transactions. The bank will contact one of the card schemes or call the police and they will then start trying to track down where the data was breached. The relevant company will receive a call from their bank, card scheme or the police advising them to look at their data files to see if they have been tampered with.

It is essential that you train senior management so that when incidents are reported to them they know what to do and can bring in the right people, including notifying your insurance broker. But you should also train anyone where there is a point of entry to the company. Tell them who exactly in the legal department they need to speak to if there is a problem. What you do not want is for there to be any delay in the breach coming to light.
You have identified the breach as a credible threat, what do you do next?

When I know there is a breach, I have a checklist in front of me covering everything I need to consider. There is a lot to think about and, of course, everyone is panicking. The CEO is calling you, he/she does not know whether it’s a £1bn or a £10 problem. As with disaster recovery, I need to have all my materials ready and my team prepared.

Your Crisis Management Committee (CMC) should be made up of senior people and needs to be prepared to meet on a regular basis. It should be separate from the Executive Committee but be in a position to provide constant updates. My CMC has always consisted of at least the Chief Corporate Communications Officer, the Chief Technology Officer (CTO), the Chief Information Security Officer, and the Chief Lawyer; sometimes others such as Head of Resources.

It is useful to have a protocol agreed so that you know who is in charge, decision levels and what steps you need to be taking. I always suggest that the Chair of the CMC should be from legal. Lawyers are suited to this, as they think in a rational and logical way. They can keep an eye on the corporate communications people to make sure they are not saying anything damaging. They can make sure the CTO hires the right external forensic team and that they are dealt with appropriately. Overall, lawyers can ensure the whole process is managed carefully and that a clear audit trail is kept.

It is also important to ensure your external teams are in place. You may normally use one external law firm, but do not rely on just one firm because when you desperately need them they may be unavailable. I have always had three law firms with two names for each. Your CTO and Communications team should also have their own experts lined up and ready. These experts should match up with the list of experts on your cyber insurance policy, whether they are your preferred experts, that you ask the insurers to write into their policy, or the insurer’s preferred experts.

Having a dress rehearsal of a breach can be an extremely valuable exercise. Bring on board senior people so that the rest of the company take it seriously.

As an in-house lawyer, how do you manage the forensics and the corporate communications team?

You use common sense. Most companies who have cardholder data will have a Qualified Security Assessor (QSA). When a breach occurs your CTO will go to your QSA because they know the systems well and can help investigate. The first thing that the CTO and QSA must do is to contain the breach.

As a lawyer, you need to look for potential conflicts. It can be a good idea to bring in a new, independent QSA alongside the existing one to ensure that nothing gets hidden. It is an extra expense but, in these circumstances, worthwhile.

With corporate communications, there is a fine line to walk. Whereas lawyers tend to be more cautious, corporate communications tend to communicate more openly and think less of the risks. Before you start saying or admitting anything, and indeed as soon as you are aware that the incident is ‘real’, you need to liaise closely with your insurance brokers and underwriters. You do not want to risk undermining your insurance where you may have to pay out millions!

There should be a communications plan in place before a breach happens. The communications team should have their external advisors ready and their internal and external messaging, questions and answers prepared in draft form. I have seen companies prepare by setting up a backup website with the necessary information about how a breach is being dealt with. The media, including social media, should be monitored so that you are the first to know if a story breaks or new facts emerge.
What are the key points on your checklist for dealing with a breach?

The high level principles at the top of the checklist are to stop the breach, analyse it and then take remedial action. Initiate the Crisis Management Committee as soon as possible. After the first meeting, I want a report, ideally from the CTO, so that we know what has happened and can report upwards. You may decide that you want someone external, such as the QSA, to produce the report for the CTO. You should have started already thinking about the issue of legal privilege and if and how to maintain it. This can be extremely complex, especially if you operate in many jurisdictions.

The next thing to consider is what data retention is required. There may be automatic systems to delete data—do we need to override the system to ensure data isn’t deleted or lost?

Consider whether it is possible to get an injunction to prevent the disclosure of data. You can get an ex parte injunction with a penal notice attached to it putting the hacker on notice if they breach it, but is it worth it since you won’t know the identity of the hacker? It may scare him/her off, but it may be a complete waste of time and expense. Consider getting an injunction or a specific order on the internet service provider to give you any information they may have on the hacker.

What type of data is involved? Is it intellectual property or is it personal or confidential data? Are you a data controller or a data processor? These are very important distinctions and will affect how you deal with the breach. For example, if you are a data controller and the breach contains personal data, are there breach notification rules in place in the jurisdiction? If there are none, do you want to tell the affected individuals anyway? This type of action can help mitigate damage to your reputation. Remember that it is not just about the breach; it is also about demonstrating the company’s competency in managing a crisis. But remember at all times, to include your insurers and bear in mind your potential legal exposure.

You then need to decide whether you need to inform the regulators. Are you required to inform them? If not, do you want to tell them anyway because it is better to tell the Information Commissioner than have them find out? If you are on a stock exchange, consider whether you need to inform them too, and indeed whether there are any other regulators to advise. Have you contacted the police and security services? You have a corporate social responsibility—and perhaps a moral duty—to tell the police who may be able to track down the criminals so it does not happen to someone else.

In addition to assessing your potential liabilities under relevant privacy legislation, assess your potential liabilities under your customer contracts. There will probably be thousands of contracts accumulated over many years and each contract will, no doubt, have a different form of liability. Nowadays, if you are providing business to business information technology services, many liability provisions relating to the loss or theft of data can be extremely burdensome. Before a breach occurs, how about doing some homework; review the liability provisions (and therefore your financial exposure) of your ten largest contracts—that is a good starting point, and gives you some ammunition to get others in the company to treat the issue seriously.

If there has been a breach then clearly something has gone wrong and you will need to conduct a post mortem. Are you going to get an external technology firm to carry this out or do it in-house? Depending on the size of the breach, your Board may weigh in. Remember that after a breach, and depending on the jurisdiction, the relevant Information Commissioner may want to carry out an audit as well as any regulator that regulates your specific activities. Assuming you provide services relating to the provision of data, and depending on what you have agreed to in your contracts, there is a good chance that your customer agreements will oblige you to let in a third party auditor following a breach. If this is the case, then hopefully you will have negotiated those contracts so that your customers are happy for you to appoint a single third party auditor. You do not want 30–40 different auditors sent by your customers!
What lessons have you learned?

Each breach is different, so there is no silver bullet in how to handle a breach. But be prepared beforehand because then at the very least you give you and your company the best possible chance of mitigating the various risks. In my view and experience, being overly legalistic or trying to avoid liability at all costs is not the right approach to a data breach. Corporate communication experts advocate the 3Rs: Regret, Responsibility and Remedy. It is about owning up and preventing reputational damage. Take responsibility and then remedy it. Keep your insurers fully informed at all times—they will be able to help as they have considerable experience of how to handle breaches. Make sure that the CEO fully understands the company’s potential legal, financial and reputational exposure.

Ultimately, you learn from the process and from what went wrong. Very often it is something stupid like not getting hold of your external lawyer or information regarding the breach not being passed on quickly enough. Like with disaster recovery, you learn to be prepared for things like this so that they do not happen again.

If you would like to discuss further any of these points addressed or have any questions on managing cyber breaches, please do not hesitate to contact a member of the Paragon Privacy, Cyber & Technology team.

Contact Us
If you would like to know more about how we can help you, please do not hesitate to contact us.

LYNDSYE BAUER
Partner
E lbauer@paragonbrokers.com
T +44 (0) 20 7280 8228

WILLIAM WRIGHT
Senior Vice President
E wwright@paragonbrokers.com
T +44 (0) 20 7280 8252

ERICA CONSTANCE
Senior Vice President
E econstance@paragonbrokers.com
T +44 (0) 20 7280 8285