How a company can survive a personal data breach

John O' Brien, Associate at Reed Smith LLP, addresses some common questions controllers will face in the wake of a personal data breach

It's happened; your worst fears have come true. Your company has suffered a personal data breach. And it's major. This is not an employee leaving a USB stick on a bus; your company has been hacked. Personal information that is core to your business is compromised. Lots of it. Your IT team is struggling to work out precisely what has happened. You may receive a ransom demand from the hackers.

You are responsible for your company's data protection compliance and your company is panicking. What do you do?

This article answers some of the practical questions you will face within the first hours of a personal data breach. These are questions that every in-house data protection team, legal team and general counsel will be expected to have answers to immediately. They may not necessarily be questions you have thought about during your General Data Protection Regulation ('GDPR') planning.

The questions

Everybody panics during a personal data breach. Even the most detailed policies and procedures will not stem the initial bout of such panic. These are the questions you will need to answer immediately:

1. What do we tell people?

Short answer: the truth. The GDPR is predicated on the concept of transparency.

If you're a consumer-facing organisation, and consumer personal data have been compromised, prepare to scale up quickly.

You need to be able to handle the deluge of phone calls, emails and tweets that are heading your way. You also need to be able to craft coherent, clear and helpful messages to affected individuals that explain what is happening.

The GDPR allows companies to notify individuals on a rolling basis. However, confusing initial notification emails and newspaper adverts will do nothing other than sow the seeds of panic among your customers. Get a handle on your external-facing communications plan. In a breach scenario, *how* you say things matters as much as *what* you have to say.

Figure out who needs to sign off on external communications. The legal, IT, executive leadership and public relations teams should all have a hand in crafting your company's message. An overly technical email won't be understood by recipients. A glossy communication runs the risk of your company not being seen to take the issue seriously.

The temptation at this stage will always be to reassure customers that everything is okay. Avoid doing this. Convey only the facts as you know them. If you think customers may have had their identities stolen as a result of the breach, tell them. Don't hide behind jargon or technical explanations.

The bottom line is that people want to know what has happened, how it affects them and what you're going to do to fix things.

Here's what you can do now to be prepared:

Plan for disasters. Have the capacity to massively scale up your call centres and social media presence. You may need to start thinking now about third party customer breach support services. The time to negotiate these contracts is now, not during a breach.

Draft a common set of FAQs. These can be published immediately when a breach occurs. Obviously you cannot predict the nature of the breach you will have to deal with. However, certain things that your customers will want to know will be common across all breach scenarios. For example, best practice guidance on how to prevent identity theft and fraud can be prepared now.

Know who your gatekeepers will be. When your company experiences its first serious personal data breach, don't be surprised when nobody wants to take ownership of the response process. Everybody will be scared to put their neck on the line and make the necessary, and

(Continued on page 10)

(Continued from page 9)

often difficult, decisions. Have a clear, internally publicised and tested escalation chain that ensures necessary information gets to decision-makers quickly.

2. Who is in charge?

Somebody has to be in charge of your company's overall response. Who should it be? The Chief Executive Officer? The Data Protection Officer? Chief Information Officer? General Counsel?

Figuring out the chain of command early is vital. Going public about a serious personal data breach can have a significant impact on a company's health. The public announcement has the potential to knock millions of pounds off a company's valuation. It can also lead to a massive loss of consumer confidence, expensive remediation efforts and lost profits. If you are not clear about who is in charge, a leadership vacuum will be created. This is the last thing that a company in a panic needs.

"The markets do not like surprises. In the short run, expect a serious personal data breach to wipe money from your company's valuation. Whether or not your company's valuation rebounds might depend on how it is seen to handle the personal data breach."

Inevitably, three teams tend to forge a company's response in personal data breach scenarios: legal, IT, and executive leadership. Your public relations team should be involved in the process but it will help craft the message rather than drive the response.

Each of these teams has an important role to play. IT needs to tell the legal and executive leadership teams what's gone wrong, how serious it is and how it can be fixed. Legal needs to tell the IT and executive leadership teams what the law requires the company to do and when it must be done. The executive leadership team needs to tell the IT and legal teams what impact this will have on the business.

Together, the teams must decide what steps the company can take given its structure, resources and level of preparedness.

Here's what you can do now to be prepared:

Establish your personal data breach control team. This team should have representatives from the legal, IT, executive leadership and public relations teams. Each representative should be a senior employee who can make decisions and speak authoritatively on behalf of their team. You need to have a personal data breach control team that can take decisions quickly as the situation develops. You need to avoid team members doubting one another's capacity to take decisions on behalf of the company.

Drill, drill, drill. Run personal data breach scenarios throughout the company. Go further. Run unannounced personal data breach drills. Get people in on a Saturday. Your team won't thank you now but they'll be glad of the preparation when the worst happens. Practice makes perfect.

3. What will this cost us?

At the end of the day, your company is a business. It exists, most likely, to make a profit for its shareholders. Personal data breaches don't add anything to the bottom line. Your executive leadership team will want to know how much this is going to cost.

It's impossible to answer this question at the beginning of a breach. To put it simply, big breaches will cost more than little breaches.

Here are just some of the costs that you'll need to factor in:

Finding out what has gone wrong. You may need to call in external IT forensic firms to understand exactly what has happened. Detailed technical expertise at short notice does not come cheap.

Notifying affected individuals. Does your marketing team have the capability to send an urgent mass communication to all your customers? Will it require outside help? Do you need to place adverts in traditional media to supplement direct communications?

Complying with the regulator's investigation. Once you've notified the relevant regulator of the personal data breach, it may commence an intense and detailed audit. It may visit your company's premises.

You will need to ensure that you can make enough staff and resources available to keep up with the regulator's pace. All of these costs must be factored into the equation before you even consider the potential fines that the regulator can hand down under the GDPR.

GDPR compensation for affected individuals. Article 82 of the GDPR empowers any individual who has suffered 'material or non-material damage' as a result of a company's infringement of the GDPR to receive compensation from that company for damage suffered. Has your company infringed the Article 32 requirement to take 'appropriate technical and organisational measures to ensure a level of security appropriate to the risk' of a personal data breach?

Providing credit monitoring. If the breach has the potential for identity theft or fraud, you're probably going to have to provide credit monitoring services to affected individuals.

Scaling up customer response channels. As set out above, you may need to engage third party service providers to deal with the surge in consumer queries. There is no worse press for a company experiencing a personal data breach than irate customers not being able to get through to call centres.

Falling share price. The markets do not like surprises. In the short run, expect a serious personal data breach to wipe money from your company's valuation. Whether or not your company's valuation rebounds might depend on how it is seen to handle the personal data breach.

Customer reimbursement costs. Your customers will expect reimbursement for any costs they incur as a result of your company's personal data breach. For example, imagine the breach compromises a customer's credit card. They need a new card issued to them immediately. Will your company pay the cost of an immediate courier? What happens if the individual is abroad at the time of the breach? Will your company pay the additional costs of an urgent foreign courier service?

Customer refunds. If your company is a consumer-facing business, your customers may be able to demand refunds for services they bought from you during the breach. Bear in mind section 49 (1) of the Consumer Rights Act 2015, which requires that "every contract to supply a service is to be treated as including a term that the trader must perform the service with reasonable care and skill". Is this personal data breach an example of your company not performing its services with reasonable care and skill?

Some of the above risks can be mitigated in advance, while others require decisions to be made as the personal data breach unfolds. Here are a few measures you can take now:

Hedge your exposure now (to the extent you can). Put a contract in place with third party service providers to provide scaled-up communications channels and credit monitoring services. You don't want to negotiate a contract to receive these services during the height of a crisis. The contract you end up with will be more expensive than it ought to be.

Be realistic about what a breach will cost. It is impossible to estimate what a regulatory fine will be, or how much consumer refunds or reimbursement costs will be, until the specific facts of a breach are known. When in doubt, err on the side of caution. As soon as the scale of the personal data breach becomes clear, start allocating sufficient resources to deal with it. Ensure that relevant decision-makers can quickly and effectively release staff and funds as required.

4. Who is going to pay?

The answer your company's executive leadership team will want to hear is: "Not us." Unfortunately, it is likely that your company will shoulder most of the costs of any personal data breach that it suffers.

Having said that, there are things that your company should have in place now:

Cyber and data risks insurance. Insurers offer comprehensive cyber insurance packages. These packages include protection against the costs of cyber extortion, business interruption, damage caused by hackers and crisis containment.

Your company can also opt to insure itself against the cost of claims made against it by affected individuals. Some insurers state that they will even cover civil penalties levied by regulators. Be careful on this point. The law generally prohibits companies from insuring against the cost of regulatory penalties. Be sure to get legal advice when negotiating your cyber insurance contract.

Vendor contracts. If your company has vendors that access its personal data, it must protect its position. It does not want to be left on the hook for the costs of a personal data breach caused by a vendor. Ensure that the contract clearly sets out the vendor's maximum liability if the vendor suffers a personal data breach that affects your customers' personal data. If necessary, carve this liability cap out of the contract's general liability cap. Get an indemnity from the vendor to ensure that financial liability is borne by the miscreant vendor, rather than your company.

Again, this is an area where your company will benefit from legal advice.

Proceed with confidence

Nobody likes a personal data breach, except maybe hackers and journalists. Personal data breaches are stressful and costly. They have the capacity to cause real and lasting damage to your company, its brand and working relationships between colleagues.

It is impossible to ever be fully prepared for the fallout from a major personal data breach. Hopefully this article has demonstrated that to be as prepared as possible requires more than standard policies and procedures. The time to start considering the issues raised in this article is now. It requires hard work, strategic thinking and a lot of banging heads together within your company. However, if the worst should ever come to pass, your company, colleagues and future self will be lining up to thank you for your foresight.

John O' Brien
Reed Smith LLP
jobrien@reedsmith.com