Media crises - preparation and prevention

Negative publicity resulting from privacy breaches is an issue no company can afford to ignore. To avoid falling into the hands of the media, businesses need to plan ahead, says **Laura Linkomies**.

In the past few years, several companies have been accused of privacy breaches in the media. In most cases, the accusations have been justified, but even the smallest incident can blow out of proportion if appropriate action is not taken.

The media reports on privacy incidents much more frequently these days. So have the risks increased, or has privacy just become a more newsworthy subject for journalists? The answer is probably both. The general public is increasingly interested in privacy issues, but on the other hand, the growth of new technologies has increased the chances of data protection breaches occurring.

However, these risks to corporate reputations can be minimised. Sagi Leizerov, a Senior Manager with Ernst & Young LLP's privacy practice, stresses that it is crucial for companies to understand the importance of perception. "The question is not whether the act was in fact offensive, but whether it is believed to be offensive by the relevant audiences."

Leizerov advises companies to prepare contingency plans for crisis management as well as establish a crisis management team. "Research into business crises in general suggests that most crises are not sudden. Privacy crises are mostly the result of management decision or indecision, a technical problem, or a human error.

"The crisis management team should be represented by several departments: IT, HR, public relations, legal operations, privacy and security. Threats can very often be anticipated, and it is down to management decision whether a budget will be provided to tackle these issues," Leizerov says.

Identify potential crises

It is vital to have a communications strategy in place in order to be able to handle crisis situations effectively. The key to being prepared is advance planning. Think what kind of privacy threats your company may face, and which are the most likely to happen. Do you collect personal data via websites? Is some of the data processing outsourced? Are there third party processors? All these factors are potential threats, and should be treated as such. But do not forget that, sometimes, all it takes for unwanted publicity is an unpopular business decision, such as outsourcing of customer data to foreign service providers.

> "The stakeholder groups who are affected by the crisis need to be prioritised in terms of their importance to the future of the organisation."
>
> - **Sagi Leizerov, Ernst & Young**

Having considered all the internal and external factors that may lead to a privacy breach, have a look at what is happening around you. Journalists use already published stories as ideas for further investigations into similar companies and circumstances. If one bank is found to unlawfully disclose personal data in an online environment, the chances are that similar cases could be found with competitors.

When things go wrong

What should you do once you have a media situation on your hands? Companies often leave admission of any wrongdoing to the last minute. However, in the long run, it is always better to admit that a mistake has been made and describe what steps the company will take to rectify the situation.

An example of defiance from a couple of years ago is the privacy case involving DoubleClick. The company was accused of not being sufficiently transparent over its data collection practices. Even when the company was ordered to pay $450,000 towards the costs of enquiries undertaken by US attorneys general, the company claimed that the settlement was not an admission of any wrongdoing.

A more serious, and still unresolved, privacy case led to the arrests of senior staff at Finnish telecoms company Sonera. At the time of the revelations in 2003, the company denied allegations that it unlawfully accessed staff and customer telephone records. But now the company's executives face criminal prosecution. The case has attracted massive media attention both in Finland and internationally, sending a host of negative messages across the world (See *PL&B International*, p.5, February 2003).

The power of apology

"Take responsibility for your actions," advises Sandy Lindsay, Managing Director of the UK-based Tangerine PR & Coaching. "While lawyers will tell us to keep quiet, nothing diffuses a situation quicker than someone 'owning up'. However, with litigation trials on the increase, there's possibly a middle ground. We could say something like: 'Our experts are telling us we are not to blame. But at present, we feel as if we

Key action points

- **Plan ahead** - Set up a privacy crisis management team and develop a strategy for handling a crisis situation.
- **Examine trends** - If privacy incidents have occurred in your business sector, the media may decide to follow up by looking into your business practices.
- **Own up to breaches** - If your company is guilty of a privacy breach, admitting responsibility will reflect far better on your organisation than a refusal to comment or acknowledge the mistake.
- **Consider stakeholder concerns** - Don't just focus on communications with the press. Consider whether you need to contact customers, shareholders or employees.
- **Brief your media teams** - Privacy incidents invariably involve complex technical and legal issues, so it is vital your PR teams are well informed.

are and, until someone confirms differently, we'll act as if we are, and do all we can to put things right.'"

Lindsay also stresses that companies should never lie to the media in a crisis situation. "It is better to try to own up to the crisis. If you've acknowledged it's your crisis, ensure you take and keep ownership of it. If you don't, someone else will – usually the media – and the real facts will be overlooked and/or distorted."

When consumer electronics firm Sony admitted a privacy breach in 1999, online services were being developed, and companies were perhaps not quite as careful and knowledgeable as today. Sony's Internet newsletter service InfoBeat had been forwarding the e-mail addresses of readers to advertisers whose banner ads the users had clicked on. The company promptly admitted that there had been a breach, and apologised.

Sometimes all you can do is apologise, but it may not be enough to satisfy stakeholders that have suffered from the privacy breach. Think of the recent case of HFC Bank, a British-based subsidiary of the HSBC financial services group, where the e-mail addresses of 2,600 customers were exposed. The company contacted the UK Information Commissioner's Office after the incident, an approach that appeared to satisfy the regulator that no further action would be needed. However, it may take time to restore consumer confidence. Although the company apologised and paid £50 to the customers whose details were unlawfully disclosed, it could face legal action from disgruntled customers (see *PL&B UK*, p 1, Sept/October 2004).

Consider all stakeholders

Often, companies are mostly worried about how bad publicity will affect their customers. However, in a media crisis, other stakeholders such as employees, shareholders and suppliers need to be kept up-to-date with developments. By releasing the right information at the right time, negative effects can be minimised.

"The severity of the crisis is not determined by the problem itself, but by the stakeholders who are affected, and how they react as a result of what has happened," explains Ernst & Young's Leizerov. "There is no business test to judge how well an organisation has survived a crisis. Ultimately, that assessment will be a perception and a matter of opinion. It will be based on how effectively the organisation communicated with its key stakeholders initially, and on an ongoing basis, until the problem was fully resolved."

Leizerov continues on the role of the media: "Public relations professionals, especially in the US and Canada, tend to think of the crisis in terms of the negative news coverage that it may generate and they consider news organisations to be the primary stakeholder group. That is a mistake. The stakeholder groups who are affected by the crisis need to be prioritised in terms of their importance to the future of the organisation. Depending on the circumstances, the news media may be a secondary consideration."

Be proactive

Your communication plan should include a list of all the people who are authorised to be spokesmen for the company. If senior management is not available immediately, it is better to have someone from the middle management to field immediate questions from the media rather than just say 'no comment'. "Never, ever, say 'no comment,'" Lindsay advises. "It means 'we are guilty – write whatever you want about us!' Being unavailable for comment gives the same message. There is always a way to say very little without saying no comment."

Lindsay also suggests that it is always best to get ahead of bad news. "If something has happened, but it's not yet leaked into the public domain, ask yourself two questions: (1) are we 100 per cent sure this won't leak? and (2) Are we 100 per cent sure that if it does, we won't be accused of trying to affect a 'cover up', which will be far more damaging than the issue itself? If not, get ahead of bad news and be the ones to break it."

"Communication should be done both by media professionals and privacy and security professionals," Leizerov says. "In some situations, the detail of the case is technical or specific, and will require the privacy or security professional's direct input to the stakeholders. In other cases the media specialist - with input from the privacy and security professional - will be the one communicating for the company with the media. Crafting the message is team work!"

Buying more time

Although the PR department will deal with the press releases, privacy professionals will be used as a source of information. While preparing a press release, PR professionals often issue a holding statement to the media explaining that the organisation is dealing with the problem, and that it will issue a fuller statement later on (mentioning the exact time if possible). This statement should be posted on the company's website, and sent to all staff who have previously been authorised to comment.

It may also be a good idea to have a 'Questions and Answers' document prepared beforehand, giving details about how the company processes personal data (similar to privacy statement on the Web). There should also be a general 'Company Profile' that can be sent out as additional information.

"The crisis could also be seen as an opportunity," Lindsay reminds us. "Anyone who has ever tried to get journalists to listen to them knows that it is not easy. But in the middle of a crisis, journalists will be straining to hear every word you have to say."

AUTHOR:

Laura Linkomies, Contributing Editor, *Privacy Laws & Business International*