# DEALING WITH A DATA BREACH
## Managing a crisis, avoiding disaster

**One day, you'll get that call.**
***"John, listen.....we've got a big problem."***
**No need to panic, you've got a data breach crisis plan in place! No?**
**If all you have are crossed fingers and a blank sheet of paper**
***- what do you do?***

Make no mistake, you WILL get that call. Just a cursory glance at the statistics shows the frequency of disclosed data breaches and the millions of records compromised on each occasion – 130m at Heartland Payment Systems in the US, 25m at HM Revenue and Customs in the UK and 6m at the Chilean Ministry of Education amongst many others, right across the world*. During a recent Websense Speakup** webinar which brought together security and communications experts, an online audience poll, revealed that 74% of participants agreed it is only a matter of time before their company's defences were breached.

So what does a comprehensive crisis plan look like? Advice from the Information Commissioner's Office (ICO) in the UK, published in 2011, states clearly that "Organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data." Following the ICO model, here are four stages to consider, with additional commentary taken from the Speakup webinar.

## Containment and recovery

As the ICO says, "Data security breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This will often involve input from specialists across the business such as IT, HR and legal and in some cases contact with external stakeholders and suppliers." So, even before you can devise a plan, the organisation's unequivocal ***commitment*** is essential. A data breach can be a minor irritation to the IT department but it can also explode into a major public embarrassment, spell financial disaster and, yes, threaten the very existence of the business. With stakes that high, the plan must be supported from the CEO downwards as it will involve every level of the business and, potentially, your own staff could be the victims...or even the criminals.

As soon as that fateful call comes in, the plan must be activated quickly. It sounds obvious but everyone should have an allocated rôle to play and they must be aware that it is time to perform. In order to provide that immediate response, the plan must:

- Designate a senior manager to manage the plan, investigate the cause of the breach and its potential effects and victims
- Allocate rôles to the necessary staff, from isolating the network to reallocating access codes
- Ensure data back-ups and disaster recovery procedures are in place

Opening the Speakup webinar, Websense's Chief Security and Strategy Officer, Jason Clark, commented that the first thing to remember is "Don't Panic!" but warned against any complacency: no attempt should be made to hide that this may be a defining point in the company's history and possibly, a number of senior management careers.

## Assessment of ongoing risk

The next part of the plan must quickly analyse the Who? What? Where? and Why? of the breach so that the appropriate steps can be taken. A minor disclosure in an email or on a social network is embarrassing but not catastrophic. A sophisticated hack which lifts your customers' credit card details or health records is apocalyptic. However, both scenarios require a measured response so the plan needs to know the following:

- Is the data personally or financially sensitive?
- Is it encrypted?
- Has the data been stolen or compromised?
- How may records have been attacked?
- Who are the victims? Customers, staff, patients?
- What are the potential consequences of this data falling into the wrong hands? What is the worst-case scenario?
- Is there a wider threat to public safety or critical services?

During Speakup, Joerg Weber, Head of Attack Monitoring at Barclays, said his bank has a comprehensive Incident Response Plan to ask all those questions in all conceivable scenarios, including an ongoing breach. He feels encryption is an important factor in mitigating the data loss but Jason Clark pointed out that if encryption is used extensively, its effect is like antibiotics - companies lose transparency and sight of underlying conditions.

In starting an analysis of the breach, Clark advises against any instinct to turn off the server. The data has probably gone but if the attack is still happening, the process can be watched and isolated. Most importantly, it can quickly show what is being taken and whether a sophisticated hacker or a mischievous amateur is at work.

## Notification of breach

Notification may give people and organisations the necessary information about a breach but a considered communications strategy is vital to averting a crisis. Depending on the type of data which has been compromised, it may be necessary, by law, to inform certain regulatory authorities. The police, insurers and bank or credit card companies can be both necessary and very helpful contacts.

However, the victims of the breach require case-by-case consideration. As the ICO says, "***You need to consider who to notify, what you are going to tell them and how you are going to communicate the message.***" Describe clearly what has happened, when it happened and what steps have already been taken to dilute the risks. A helpline or web-based service can provide further information in the days after the incident. However, if a breach only affects a handful of people, consider the downside of informing everyone: tailor the response!

If the breach is sufficiently high-profile, the media may soon become interested.  An informative and calm response to journalists' enquiries is essential so communications management and public relations agencies must be 'in the loop' at an early stage.

Discussing communications during Speakup, Matthew Mors, Vice President at MIX Public Relations in Seattle, added that the European Union is proposing regulations which cover data outside the EU market so, for example, a US company would need to involve authorities if EU customers are involved. Also in the US, the Securities and Exchange Commission has to be informed if an incident might affect a company's stock value.

Jason Clark noted that the decision to involve law enforcement should be a defined point in any crisis plan. Once the police are involved, the incident could become public information so this can be a reason for discretion if the breach does not have to be disclosed legally.

## Evaluation and response

If there is any silver lining in a data breach incident, it is that weaknesses in data security are exposed. A systematic review of policies and responsibilities should be part of any plan to avoid making the same mistake again. Focus on tightening your response in these areas:

- Be clear where, and how, your sensitive data is stored. Is it concentrated in one location or spread across the enterprise?
- Sharing data is always a key vulnerability, whether online or by physical means such as a USB stick. Minimise those transactions!
- The human factor can never be underestimated. Security awareness training could be your best investment.

The final Speakup comments added some concluding thoughts on the insider threat and on technology. Jason Clark observed that threats do not always come from outside and internal controls are a wise part of any data loss prevention plan. For example, when a manager gains additional access rights through a promotion, a little extra vigilance on their IT activity would be prudent, as well as any personnel with a wide range of access. Anomalies in behaviour such as accessing unusual files or databases can be significant as is the use of a generic email address rather than the corporate system. It may even be reasonable to allow limited fraudulent activity to monitor patterns and behaviour.

Finally, on technology, Clark says that AV and firewall data protection is no longer enough and newer, better technologies exist. It is imperative that you look for innovation technologies that stop DATA Theft and Advanced Malware. Joerg Weber agrees that, whilst he is confident that Barclays has comprehensive cover, there is no one ideal system. Every organisation must find the right mix at the right cost for its individual needs.

Whether you're on the front line in a bank, advising on communications or delivering IT security, the message is clear:  a data breach should not become a disaster. With a well-devised plan, you can manage the crisis!

*Nathan Yau, flowingdata.com

**Websense Speakup: "Dealing with a data breach. Managing a crisis, avoiding disaster."  9 February, 2012

*If you would like to comment on this article or start a discussion on other information security topics, then join us on the LinkedIn SpeakUp group – Websense SpeakUp.*

**About SpeakUp**

SpeakUp is a forum to discuss the issues facing security professionals today. The SpeakUp webcasts and live events are professionally hosted and consist of a panel of experts from the security industry debating and addressing the latest issues with an audience of security professionals.

In short, SpeakUp is the BIG security conversation.

Learn more at **www.websense.co.uk** | **0808189 0367** | **info-intl@websense.com**