Getting to know you
Reputation &

Protecting personal data is now a top priority alongside physical measures needed to help people feel safe.

How do you protect your reputation when their details are stolen from you?

How much personal information would you be willing to give away for a pint and a bhaji?

Suddenly, in the COVID-19 world in which we now live, surveillance and monitoring technology will be vital in helping to thwart the virus – and against our better natures we are being forced to give away basic details just to be able to do day-to-day activities such as visiting a restaurant or pub.

The hooha around the adoption of the EU's General Data Protection Regulation (GDPR) in 2018 meant the public became far more aware of how their data could be used. Certainly, in the UK, the ever-increasing number of cyberattacks on organisations and individuals have given rise to a noticeable reluctance to share details because of concerns about security.

Your data is valuable

Data is big business for hackers, particularly sensitive health information. According to CISCO's Benchmark Report 2020, the number of organisations reporting reputational damage from data breaches has risen from 26% to 33% in the last three years. As we've seen with high profile attacks, it is not so much the breach itself but the way in which it is handled that can rapidly turn it into a reputational and financial disaster.

When Uber realised that hackers had accessed personal data of 57 million customers and drivers in 2016, they made the costly mistake of trying to cover it up. Instead of reporting it, they paid the hackers $100,000 to delete their ill-gotten gains and keep the breach quiet. Not only did this not work, it was against the law. They were fined £900k by the British and Dutch regulators and suffered a huge blow to their reputation.

The GDPR allows you 72 hours to disclose the breach and fines are now much bigger. Last year British Airways faced a record £183m fine from the Information Commissioner's Office (ICO).

In addition to losing trust in an organisation, outraged customers will be quick to go online and share their experiences with others. This in turn will attract negative press, impact brand value and result in customers going elsewhere. In Uber's case, their reputation suffered further when customers launched their #DeleteUber campaign and competitors were quick to challenge their marketplace lead.

Acknowledge the risk of a cyberattack

Data breaches are occurring every day, and all of us – whether an individual, SME or global organisation – need to acknowledge that a cyberattack is almost inevitable. You will not only need IT solutions to protect the data; you also need a robust Crisis Media Strategy (CMS) to help protect your reputation.

When sensitive data is stolen

All your staff should know what constitutes a breach and, as part of your Business Continuity Plan (BCP), should know what to do if there is one. They should also understand the need to communicate what is happening as quickly and truthfully as possible with the help of your CMS.

A section on cyber breaches should have its own templates and procedures for communicating the incident internally and externally, as well as up-to-date contact details for all stakeholders and any external agencies that need to be alerted.

It is vital that you are seen to care about your customers. Once you have contacted them, you need to immediately issue a public statement via your website explaining what has happened, what data has been affected and how you are handling it. Most importantly, you need to explain what customers should do to protect themselves.

Your phonelines, network connections, software etc. can all be compromised in an attack, so make sure you have back-up lines of communication so that you can talk to those affected and they can talk to you. These can include using the press and social media.

Monitor and respond as necessary to any negative online chatter to nip rumour and speculation in the bud. Your CMS should also detail how and when to respond to press inquiries; I recommend as soon as possible to avoid an information gap and ensure that you are the source of the most up-to-date details on the situation. Transparency goes a long way in the reputation stakes.

Tips for the future

Review your BCP to ensure that new cyber risks from increased remote working, video conferencing, personal devices and Wi-Fi and use of corporate emails for social activities are thought through and explained to your staff.

Communication is key to providing reassurance that your customers' data is safe:

- **Make it clear that you are compliant with GDPR on your website and other communiqués.**
- **Unless you are exempt, no matter the size of your organisation you must pay a data protection fee to the ICO if you collect any personal data.**
- **Where possible make data security part of your values to demonstrate you can be trusted.**
- **Let your customers have control over what information you keep, how it will be used, the advantages to them and for how long it will be stored.**
- **Ensure you have their consent to share it with third parties.**

Invest in proper media training and regular resilience tests for all spokespeople and public-facing staff such as telephonists, receptionists and security. A media-trained cyber expert can explain often complex detail in layman's terms.

As for giving YOUR details to strangers, be wise. If it feels like they are asking for too much, they probably are!

If you are uncertain about GDPR, your obligations and how much information to provide, the ICO website (https://ico.org.uk/) is an excellent resource.

Anna Averkiou
Journalism TV Radio Online Training Media Strategy Crisis Management

www.averkioumedia.co.uk