TRAVELERS

Protecting your reputation in an age of cyber breaches

Technology thought leadership

Contents

Reputation and brand go hand in hand

In an age when a negative post can go viral and reach millions of people in a few hours or days, reputation management is moving to the forefront of corporate concerns.

Companies should consider the advice of Socrates more than 2,400 years ago: "Regard your good name as the richest jewel you can possibly be possessed of – for credit is like fire; when once you have kindled it you may easily preserve it, but if you once extinguish it, you will find it an arduous task to rekindle it again."

Socrates could not have envisioned the speed with which a good name can be lost today, but he would not have been surprised by the consequences for businesses: lack of trust and loss of customers. This is particularly true when the source of distrust is a data breach that has exposed private information that customers expect to be guarded carefully.

Unfortunately, data breaches have become common enough that all businesses that collect information need to worry not only about safeguarding their data, but also about protecting their reputation.

The Information Commissioner's Office (ICO) says: "Under the Data Protection Act, you have responsibilities to protect the personal information that you and your staff collect and use. Breaches of data protection legislation could lead to your business incurring a fine – up to £500,000 in serious cases. The reputation of your business could also be damaged if inadequate security contributes to high-profile incidents of data loss or theft." [i] In 2018, the General Data Protection Regulation will introduce new data processing and notification requirements. For example, data controllers are required to notify the ICO (or equivalent) within 72 hours where there is a data protection breach. Breach of requirements relating to international transfer of data can result in fines up to 4% of worldwide annual turnover.

In this report, we discuss the risks around data breaches and how you can protect your organization, including:

- Why reputation matters
- Whether data breaches are a risk for your company
- Companies hitting the headlines
- How to protect your reputation

We hope that you will find this report useful and would welcome any feedback.

Mark Crane
Technology Practice Leader
Travelers
mcrane2@travelers.com
+44 (0)20 3207 6232

"Regard your good name as the richest jewel you can possibly be possessed of."

Why reputation matters

A mention of Bentley conjures up images of high-end luxury. See the Apple icon and sleek, innovative technology comes to mind.

These iconic brands are valuable to their companies because customers see them as representing positive attributes that build trust – and trust leads to sales.

Unfortunately, the opposite is also true. When a brand becomes associated with negative messages, the damage in the marketplace can be extensive and long lived. (One example was the fall in sales of Toyota cars after reports of crashes caused by sticky accelerators). A poor reputation can even impact the ability of a company to attract and retain a talented workforce; no one wants to work for a company with a bad reputation.

The erosion of a brand can come from any number of directions, including substandard products, poor customer service and lack of social responsibility, to name but a few.

Increasingly, data breaches can also create negative attention for a company, often leaving customers believing that their information has been mishandled because of corporate indifference to protecting their privacy and financial information.

A 2012 Financial Times article pointed to the growing sensitivity of customers, alluding to a survey by PR firm Edelman which found that 70 per cent of customers are more concerned about data security and privacy than they were five years ago, and 85 per cent think that companies need to take protecting data more seriously than they do.

"When a brand becomes associated with negative messages, the damage in the marketplace can be extensive and long lived."

Are data breaches a risk for your company?

If your company collects and stores data, a data breach is always a distinct possibility.

Consider the following statistics:

- In the government and PwC 2015 Information Security Breaches Survey, it was found that 90 per cent of large UK organizations had suffered a security breach in 2015 (up from 81 per cent the year before).[ii]
- The survey found that 74 per cent of small organizations had suffered a breach, up from 60 per cent in 2014.[iii]
- The survey also found that the costs associated with data breaches had risen sharply for UK companies employing more than 500 people to between £1.46 million and £3.14 million per incident.[iv]
- In a global study, IBM and Ponemon Institute found that the average total cost of a data breach had increased to approximately £2.63 million.[v]

Despite the large number of data breaches reported, experts agree that many breaches are never reported, meaning the figures above – as large as they are – fall short of reality.

- In addition, it is worth noting that suffering a data breach once is no vaccine against further occurrences. In the government/PwC research, it found that the median number of security breaches for large organizations was 14 breaches in a year for large organizations and four breaches for small organizations.[vi]

Making headlines for all the wrong reasons

Companies hitting the headlines because they have been victims of data breaches are almost too numerous to mention.

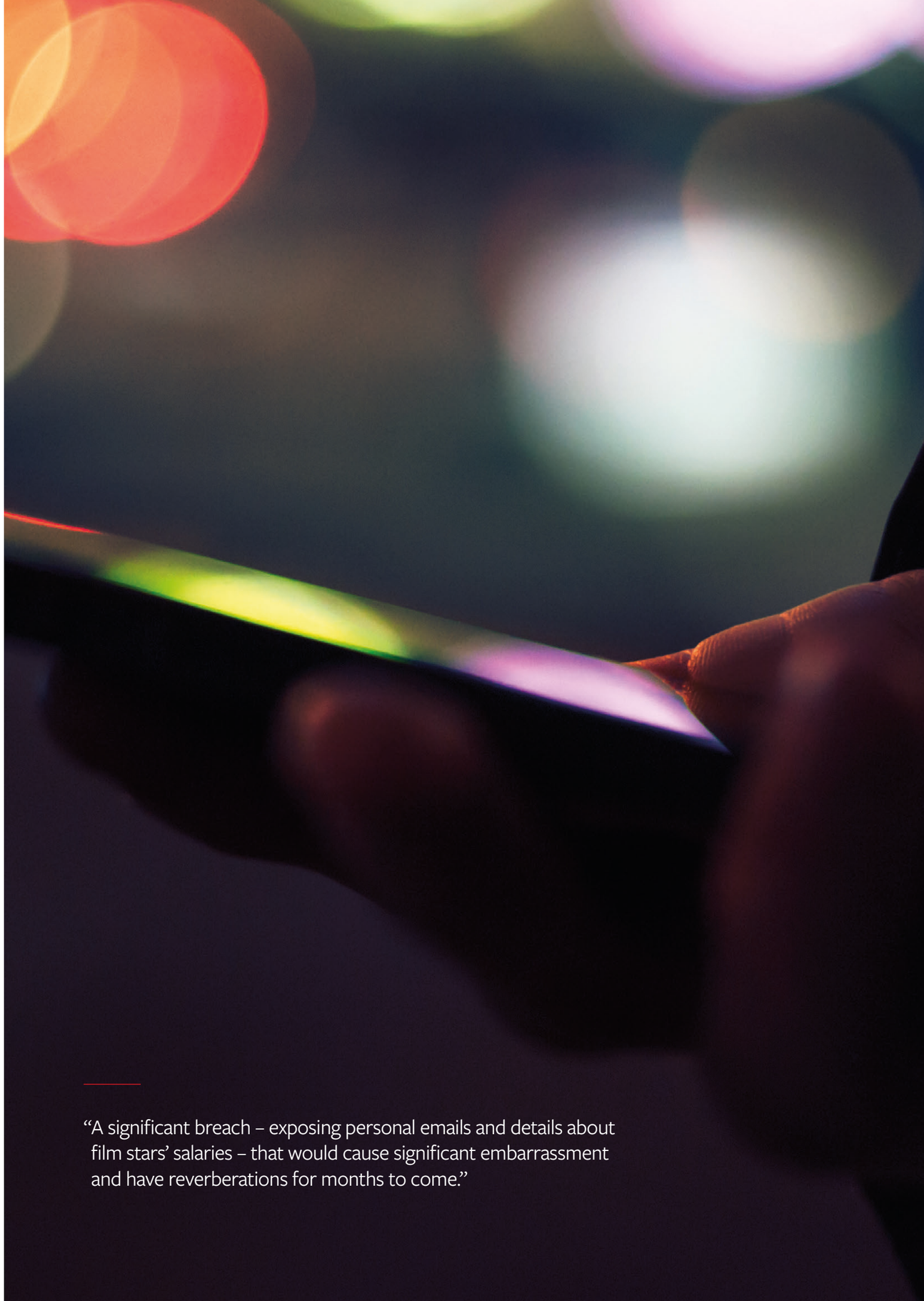
Examples include the high-profile TalkTalk hack in October 2015, during which more than 150,000 customers' details – including their bank account numbers and sort codes – were stolen.[vii] The company told the BBC that the hack was likely to cost them up to £35 million.[viii]

Also in October 2015 came a reminder that not all data breaches are due to malicious hacks: Marks and Spencer apologised to customers after its website experienced a technical error that allowed customers to see each other's personal details when they logged in.[ix]

The same month, British Gas warned more than 2,000 of its customers that their personal details had been published online – although it could not explain why as it said it had not been hacked.[x]

Earlier in the year, unfaithful spouses everywhere had cause for concern when Ashley Madison – a global dating site for married people – was hacked and information about its 33 million users was reportedly published on the 'dark web'.[xi]

In one of the most high-profile data breaches of recent years, Sony Pictures experienced a significant breach of its internal computer system in late 2014 – exposing personal emails and details about film stars' salaries – that would cause significant embarrassment and have reverberations for months to come.[xii]



"A significant breach – exposing personal emails and details about film stars' salaries – that would cause significant embarrassment and have reverberations for months to come."

Protecting your reputation

However, bad things can happen to good companies – especially when it comes to data integrity in an era of pervasive hacking, viruses, spyware and malware. Therefore, it is important to be prepared to defend your company's image.

The following steps include both proactive and reactive measures for maintaining your reputation.

Assess your risks
Understand the risks to your reputation, whether from data breaches, product failures, customer complaints or social media attacks. Identify your assets that can be called into action to defend or repair your reputation.

Form a response plan
Create a plan for handling a negative event, including creating an Incident Response Team. If a data breach occurs, what steps will the company take first? Who will notify authorities, handle the media and liaise with customers? What resources are available to handle the extra workload and provide the expertise to address the situation? The plan should lay out timelines and responsibilities so that certain key decisions do not have to be made in the heat of the moment.

Transfer your risk
As for any other type of risk, a company should look for ways to transfer the risk of suffering a data breach. Many types of insurance today include coverage for cyber incidents. Look for a policy that pays for reputation management and PR services.

Build relationships
To avoid a steep learning curve in the midst of a crisis, develop relationships in advance with companies who can provide reputation management assistance. Firms that specialise in brand management can help a company to recover from a data breach, especially if they are brought in during the proactive planning stage before a crisis occurs. Make sure that any partners understand your company's values and goals, as well as your market position and brand value.

Put a communications plan in place
Effective communication is critical during times of crisis. The first few hours and days can make a significant difference in how customers and the public perceive a company. Is the company transparent, forthright and responsible? Or is there an attempt to gloss over facts, hide pertinent information and deflect blame?

The UK government also provides a wide range of guidance to help companies large and small to manage their cyber risks effectively. Companies should familiarise themselves with the Cyber Essentials scheme and consider seeking Cyber Essentials accreditation, which can go a long way towards minimizing your risks around data breaches.

What customers want to know

The US' Online Trust Alliance[xiii] says that customers want to know the following after a data breach:

- Incident description – what, how and when?
- What type of data was breached?
- Who is impacted – number and type of customers?
- What action is the business taking to help affected people?
- What steps are being taken to make sure it does not happen again?
- What is being done to stop fraudulent use of the stolen data?
- How can customers get more information?
- What are the next steps, and how will the company keep customers informed?

Sources and further reading

2015 Cost of Data Breach Study: Global Analysis, IBM and Ponemon Institute
http://www-03.ibm.com/security/data-breach/?ce=ISM0484 &ct=SWG&cmp=IBM-Social&cm=h&cr=Security&ccy=US& cm_mc_uid=50638836157114610739149&cm_mc_sid_50200000=1461073914

ICO (Information Commissioner's Office)
https://ico.org.uk/

Cyber Essentials scheme overview, government
https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

10 Steps to Cyber Security, government
https://www.gov.uk/government/publications/cyber-riskmanagement-a-board-level-responsibility/10-steps-summary

Online Trust Alliance
https://otalliance.org/resources/ incident/2012Data-BreachGuide.pdf

i https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf

ii https://www.pwc.co.uk/assets/pdf/2015-isbs-technicalreport-blue-03.pdf

iii http://www.pwc.co.uk/assets/pdf/2015-isbs-executivesummary-digital.pdf iv https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf v https://securityintelligence.com/cost-of-a-data-breach-2015/

vi http://www.pwc.co.uk/assets/pdf/2015-isbs-executivesummary-digital.pdf

vii http://www.bbc.co.uk/news/technology-35425275

viii http://www.bbc.co.uk/news/uk-34784980

ix http://www.theguardian.com/business/2015/oct/28/marksspencer-shuts-down-website-due-to-technical-glitch

x http://www.telegraph.co.uk/technology/internet-security/11962771/British-Gas-data-leak-is-third-major-UKsecurity-breach-in-a-week.html

xi http://www.bbc.co.uk/news/technology-35101662

xii http://www.bbc.co.uk/news/entertainment-arts-30512032

xiii http://otalliance.org/resources/incident/2012Data-BreachGuide.pdf

About Travelers

Here is a comprehensive list of the covers we provide and the types of business we provide them for.

Products

Business Interruption

Crime

Criminal Protection Response

Cyber (1st & 3rd party)

Directors & Officers

Employers' Liability

Employment Practices Liability

Event Cancellation

Kidnap & Ransom

Personal Accident & Travel

Professional Indemnity

Property

Products Liability

Public Liability

Terrorism

Industries

Advanced manufacturing

Automotive

Educational services

Financial institutions

Healthcare

Hotels

Legal

Marine

Media and entertainment

Professions

Public services

Retail

Transport

Real estate

Technology

Warehousing and distribution

TRAVELERS