



Data Breach Readiness 2.0

The 'Customer First' Data Breach Response

A rapidly changing landscape means a radical rethink for UK businesses.

An Experian Whitepaper

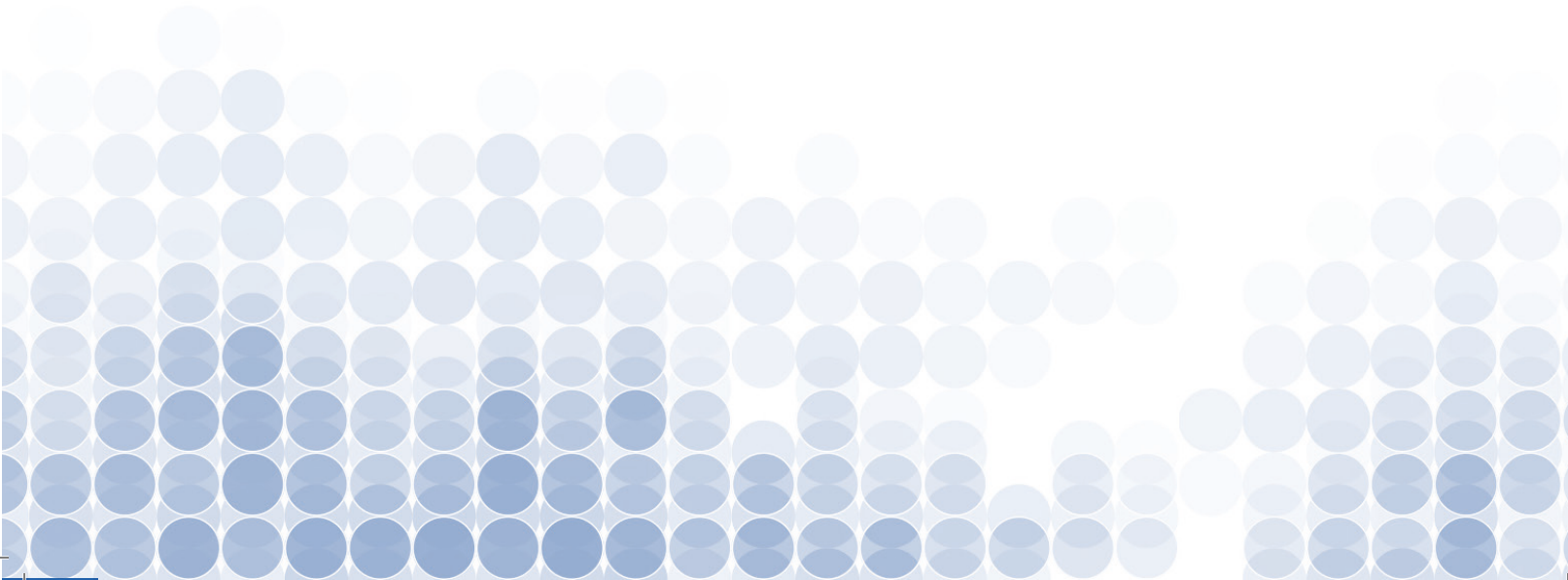


Table of Contents

Introduction.....	3
In Summary	3
The UK Data Breach Landscape.....	4
2014: The Year of the UK Data Breach?.....	4
The Customer Impact: A Financial Halo Effect	5
The Customer View	6
The Halo Effect.....	7
The Business Response: Ready for Anything?	7
Trial and Error.....	8
Looking Ahead: The Future of Data Breach in the UK	9
The US: A Precursor for the UK?.....	10
Where we're heading: The expert view - key considerations across the data breach response ecosystem.....	12
Customer Support: Protect Customer Relationships.....	12
Insurance: Look Beyond Liability	12
Legal Counsel: Navigate the Complexity	13
Digital Forensics: Secure the Evidence.....	13
Crisis Communications: Care, Concern, Commitment.....	13
Conclusion	14

Introduction

The data breach landscape in the UK has changed beyond all recognition over the last few years. More than four in ten Britons (42%) have been affected in some way by a breach, and their levels of concern are growing.

Cybercrime has become increasingly complex and sophisticated, and unprecedented levels of personally identifiable information are being traded illegally on the dark web. More than 110 million pieces of information were traded in 2014 alone, a 300% increase since 2012. And in one single day in February 2015, more personally-identifiable information was traded illegally on the dark web than in a three-month period in 2014¹ – suggesting the situation is set to worsen further this year. This is mirrored by the rapid growth in identity-related crimes in the UK; identity fraud now accounts for 46% of all fraud attempts².

Data breaches have become far more expensive to deal with. According to research from the Ponemon Institute, the average cost of dealing with a data breach has risen by 26% since 2011, having risen by just 3% in the preceding three years³.

But these changes could well be just the beginning, and the data breach issue is likely to accelerate over the next two years: A perfect storm of tougher regulation, increasingly negative public sentiment and rising costs will leave organisations of all shapes and sizes in no doubt that being prepared to respond quickly and effectively is no longer a matter of choice.

But how well are UK organisations equipped to cope with what may amount to a watershed in the UK data breach landscape?

This paper sets out to answer that question. It draws on results from an original business and consumer research study commissioned by Experian, and commentary from lawyers, insurers, customer support specialists, crisis communications consultants, and digital forensics experts:

- Litmus testing attitudes to data breach: To understand how UK organisations see the risk and likely impact of data breach on their organisations and customers, and to assess the extent to which those perceptions are reflected in genuine organisational preparedness;
- Quantifying the damage data breach can cause: The halo effect created when short term response and reparation costs are amplified by the longer term impacts driven by reputational damage, reduced trust and increased customer churn;
- Assessing the future of the UK landscape: Drawing on predications from credible experts from across the data breach response ecosystem, and looking to the US market for a potential glimpse of the future;
- Setting out future data breach response best practice: As described by subject matter experts from across the data breach response ecosystem.

In Summary

Overall, this paper identifies a misplaced confidence among UK organisations. While they claim to understand the risks, they are inadequately prepared to cope with the full impact of a data breach today, let alone in a future of tougher regulation in which customers really will vote with their feet.

It concludes that the organisations best equipped to cope with a changing data breach landscape will rethink readiness. They will recognise that the impact of a breach will increasingly be defined not by its size, but by the quality of the organisation's response, and their readiness plans will start with the customer, to:

- Enable a rapid and organised response, guided by a new understanding – managing customer impacts is the first step to mitigating regulatory, financial and reputational damage;
- Anticipate and pre-define responses to a wide range of data breach scenarios;
- Draw on a range of expert support to deliver a single unified response solution with customer protection at its heart.

1. Analysis carried out every six months by an independent security consultant on behalf of Experian

2. According to CIFAS, 2014

3. Ponemon Institute Cost of Data Breach 2014

The UK Data Breach Landscape

“It doesn't matter whether you are big or small. If you have an IP address and are connected to the internet, you are fair game as far as hackers and cyber-criminals are concerned.”

Nick Prescott, Information Security Manager, Blackthorn Technologies

Dubbed 'The Year of the Data Breach', 2014 saw a steady stream of serious, in some cases record breaking, data breaches hit the headlines. Some of the world's major household names were hit by cyber-attacks but, although many of those breaches will undoubtedly have affected UK customers, none of the top breaches in terms of the volume of exposed records involved UK-specific organisations.

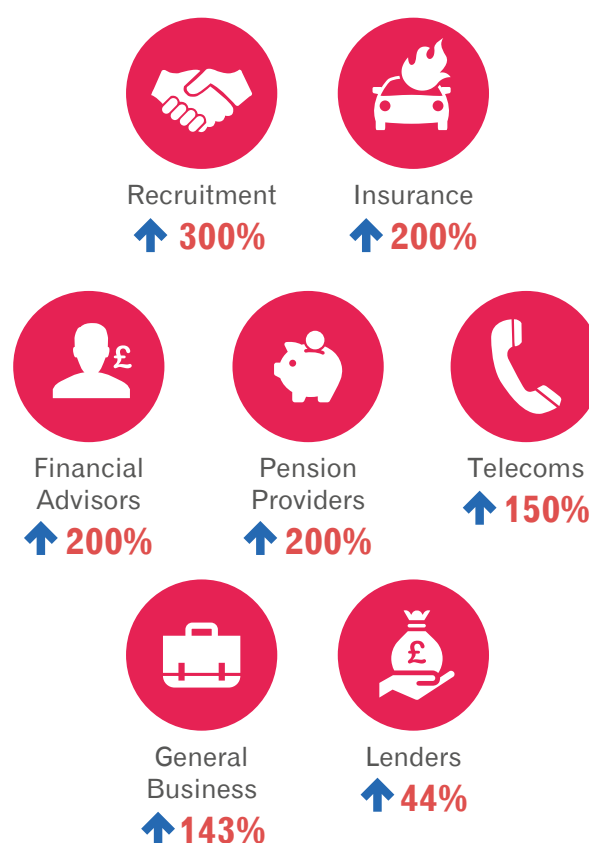
So, was 2014 'The Year of the Data Breach' in the UK and, more importantly, how has the seemingly endless procession of data breach cases during the last 12 months changed both business and public perceptions?

2014: The Year of the UK Data Breach?

There is ample evidence to suggest that the UK market did indeed follow the upward global trend.

Research commissioned by Experian and carried out by Comres, found that almost one fifth of UK organisations (17%) suffered at least one breach in the last two years. Meanwhile, over the course of the year, the Information Commissioner's Office (ICO) issued warnings to a number of sectors, including the legal and healthcare professions, pointing out that data breach incidence was steeply on the rise. In its annual report for 2013/14, the ICO also revealed that it had "...been processing record numbers of complaints, answering more questions on our help line, and concluding more enforcement actions than ever before."

Finally, a Freedom of Information Request from Egress Software also revealed a surge in the number of reported data breaches in the UK – comparing reported breaches between April and June 2013, and the same period in 2014. The figures obtained from the ICO – which also suggested a "worrying increase in data breaches as a result of human error" - showed that data breach events were on the rise across the board; for example:



It is fair to say, then, that 2014 may indeed have been the year of the data breach in the UK – but, at the same time, the steep rise in breach events did not perhaps garner the kind of media coverage that can help to increase organisations' awareness and encourage them to take the risks seriously.

In fact, most breaches that become public knowledge in the UK affect big, US-based global brands and take place in jurisdictions like the US, where mandatory notification practically guarantees media coverage. The converse is true in the UK. We have seen an upsurge in the rate of UK businesses affected by data breach but media coverage of UK-specific breaches has been minimal - arguably because notification is, for the most part, not mandatory.

The Customer Impact: A Financial Halo Effect

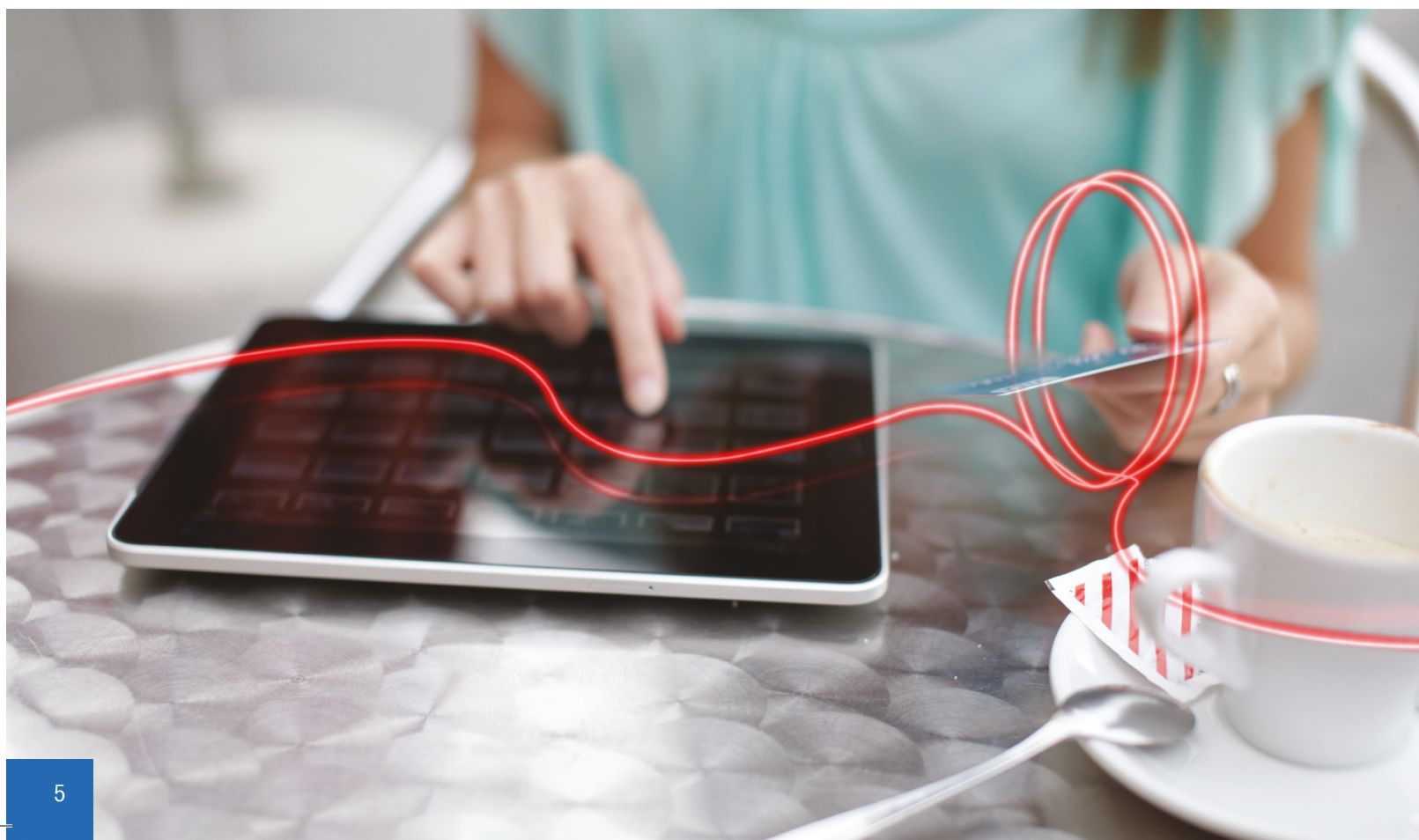
“The big thing right now if you look at any data breach is the PR downside, the impact in terms of reputational damage, customer churn and ultimately lost revenues. Our customers tend to be at the forefront when it comes to breach response, but eighty per cent of the businesses we talk to are most concerned about protecting customer relationships following a breach, with very good reason.”

Paul Bantick, UK TMB Focus Group Leader & Underwriter, Beazley plc

Whether or not UK organisations fully appreciate the risk that they will be affected by a data breach, it is clear that the majority do understand the likely impact if the worst should happen.

According to the research, they are well aware of the regulatory impact of a data breach, the cost of recovery and, perhaps most importantly, the potentially devastating effects on trust and customer loyalty. According to the research:

- 80% of UK organisations are concerned at the prospect of legal or regulatory action following a data breach;
- 84% are concerned that customers will trust the organisation less;
- 81% are concerned about the financial impact of recovering from a breach;
- 79% are concerned that customers will stop using the company.



The Customer View

“Businesses suffering breaches have maybe had a bit of an easy ride from consumers until now, but that is changing. Increasingly, I think the effectiveness of the response is what an organisation will be judged on. If they are found wanting, that is where the reputation will suffer, not just because the breach happened in the first place.”

Claire Snowden, Director, Regester Larkin

These fears are well founded. The potential regulatory impacts – from fines and reparations to the costs associated with remedial action – are well known, but changing consumer attitudes could drive more far-reaching and persistent damage.

The research found that the UK public is very conscious of the risks posed by data breaches. People are, in general, concerned about them, and agree that their perception of a business would change if it was affected by a data breach that compromised their personal information. What's more, it seems that being affected by a data breach could be likely to convert a significant number of customers into 'brand detractors', who would amplify negative reputational effects by advising friends and family against the organisation.

According to the research:

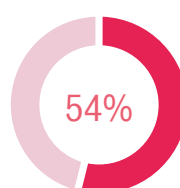
- 64% of British adults are concerned about falling victim to a data breach in the future;
- 80% say their level of trust would decrease if a company lost their personal data;
- 63% of British adults say they are likely to leave an organisation if a data breach occurred;
- 67% would advise friends and family against the organisation.

Overall it seems that customer perceptions of data breach are on the move. Consumers are less understanding, and less willing to see organisations affected by data breaches as 'victims'. Rather, they increasingly believe that data breaches come as a result of the organisations' own failures – failures in procedures, security and data controls.

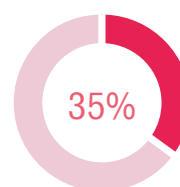
The research findings clearly bear this out:

- 90% of British adults think companies should educate their employees on data security;
- 88% think companies should have measures in place to prevent a data breach;
- 84% think companies should be penalised for compromising their customers' personal information;
- 83% think companies should be subject to increased regulation to better protect customers.

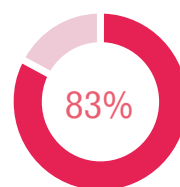
While consumers have clear attitudes as to accountability for the protection of personal information, this is further underpinned by a widespread apathy towards protecting their own information online, even in the event of being notified of a breach – making the potential end results of becoming victim of a data breach even farther-reaching.



54% of those affected didn't change the password on the affected online account when notified of a breach;



Just 35% changed the password on other online accounts;



83% made no change to their online behaviour at all after being notified of a data breach.

The Halo Effect

“We have already reached a situation where the cost of lost business following a breach accounts for almost half of the overall financial impact. This financial ‘halo effect’ has grown rapidly over recent years and will continue to do so. This is an issue that businesses simply cannot afford to ignore.”

Jim Steven, Head of Data Breach Services, Experian

This increased public awareness of data breach, the likely heightened effect on reputation and customer loyalty, as well as the multiplying effect of ‘adverse advocacy’ adds a new dimension to the financial impact of a data breach – creating a ‘halo effect’ of financial and reputational implications.

That is, organisations affected by data breach who have not adequately prepared will increasingly suffer costs associated with lost business as well as the direct cost of fines and data breach response activities. Indeed, according to the Ponemon Institute’s Cost of Data Breach 2014, this indirect cost of lost business now accounts for around 43% of the total cost of a data breach. The Ponemon report concluded that:

- On average lost business costs associated with “...abnormal turnover of customers (a higher than average loss of customers for the industry or organisation), increased customer acquisition activities, reputation losses and diminished goodwill” stood at £950,000;
- The total average cost of a data breach, including costs like breach detection, escalation and response costs was £2.21 million.

This ‘halo effect’, then, almost doubles the total financial impact of the average UK data breach – what’s more, the costs associated with consumer action and reputational damage have risen rapidly over recent years. According to Ponemon Institute figures, lost business costs have increased by 22% since 2011.

The Business Response: Ready for Anything?

The research tells a two-part story about UK business’ readiness to respond to data breaches. In essence, it is a story of misplaced confidence, and response plans built up by a costly process of trial and error.

On the surface, businesses are broadly confident. When questioned, they suggest they are well prepared to respond to a data breach:

- 79% believe their organisation is prepared to respond to the theft or loss of sensitive and confidential information that requires notification to victims and regulators;
- 81% believe the organisation understands what needs to be done following a data breach to prevent the loss of customers’ and business partners’ trust and confidence;
- 76% say the organisation understands what needs to be done following a material data breach to manage negative media or public sentiment.

Look below the surface at real plans and readiness, however, and the picture is far less positive. The reality is that preparedness is patchy at best and all important customer engagement is almost an afterthought:

- 34% do not have data breach response plans in place, and even of those who do, those plans are less than comprehensive – a quarter do not include specialist crisis communications (23%) or legal (27%) support, and almost two thirds (63%) do not include digital forensics;
- Only one third (33%) have specific budgets set aside to deal with data breaches;
- Less than two-thirds (61%) have reporting procedures in place for lost data or devices (e.g. company laptops or phones);
- Less than half (43%) have data breach or cyber insurance policies in place;
- Just 47% would notify customers ‘as quickly as possible’ following a data breach;
- Less than a quarter (21%) would offer an identify protection service to existing customers, and only 10% would offer a credit monitoring service.

The fact that data breach response planning and readiness is so patchy perhaps explains why so many UK organisations affected by breaches go on to be affected again, at least once, within two years; 57% according to the research.

“ In terms of readiness to respond to a data breach effectively, I think the average UK business scores about 5.5 out of 10. They know it's an issue but those who have not yet suffered a breach really do not understand what a massive problem it can be. There is still a lot to learn. ”

Margaret Tofalides, Partner and Head of UK & EU Data and Cyber Security Practice, Clyde & Co LLP

Trial and Error

“ We've seen companies go into a breach situation without an effective response plan in place. They are essentially learning in live situations, and pretty quickly come to appreciate the full implications of a breach and the complexities involved in a breach response. You can be sure they had plans in place the next time around. ”

Michael Bruemmer, VP, Consumer Protection at Experian Consumer Services, US

It's evident that UK organisations are underestimating the complexities in planning for and delivering an effective and well-rounded data breach response, until it is too late. This is borne out by the research findings, which clearly demonstrate improved planning and readiness amongst organisations that have already been affected by a breach. In essence, it suggests that UK businesses' data breach response planning is an iterative process of trial and error:

Planning and readiness steps	Breach in the last two years	No breach in last two years
Increased investment in security technologies in order to be able to detect and respond quickly to a data breach	81%	51%
Invested in data breach or cyber insurance policies	80%	35%
Board of directors, chairman and CEO informed and involved in plans to respond to/manage a possible data breach	91%	66%
Data breach response plan in place	93%	60%
Specific breach response teams in place	86%	59%
Specific budgets set aside for dealing with data breaches	83%	22%
Retainer or master service agreement with third-party firms that help them prepare and respond to data breaches or security incidents	86%	37%
Customer service personnel trained on how to respond to questions about a data breach incident	91%	48%

Looking Ahead: The Future of Data Breach in the UK

“The data breach landscape is going to change a great deal, and very quickly over the next year. I'd expect to see notification as a mandatory requirement for everyone by 2016, so cyber security, data compliance and breach readiness will have to become absolutely routine business practice. Right now, there is still a lot to learn.”

Margaret Tofalides, Partner and Head of UK & EU Data and Cyber Security Practice, Clyde and Co LLP

As hackers and cyber criminals become more sophisticated and internet connectivity becomes ever more ubiquitous, so the risk of data breach will inevitably rise – and rise quickly. This is the harsh reality facing UK organisations that are already behind the curve when it comes to understanding data breach risks and planning effective breach responses.

Tougher regulation, whether driven by the EU or the UK seems inevitable given public demand - 83% of consumers think companies should be subject to increased data breach regulation. Meanwhile, compulsory notification would have the added effect of raising public awareness of breaches in general – and expanding the halo effect far beyond just those affected by a breach.

Indeed, the EU Data Protection Regulation, which looks set to be introduced across all the EU member states from 2016, promises to be a game changer. It sets out a series of provisions that will fundamentally change the data breach landscape – raising both the financial and reputational stakes significantly.

Key provisions include:

- Universal mandatory notification: All Data Controllers must notify ALL breaches of personal data to the Data Protection Authority within 72 hours;
- Massively increased sanctions: Fines in the UK will rise from the current maximum of £500,000 to £100 million or up to 5% of annual worldwide turnover in case of an enterprise, whichever is greater.

These changes will raise the media and public profile of data breaches. In so doing, they will precipitate greater reputational damage and increase the impact of data breaches on consumer trust and loyalty in the future – changes that, notwithstanding its significant structural differences from the UK, have already been witnessed in the US.

As Paul Bantick, UK TMB Focus Group Leader & Underwriter, Beazley plc pointed out: “Here in the UK, certain things that have taken place in the US have not yet happened. The key thing is regulation. What that regulation does is make breaches far more complex to manage, a bigger crisis and much more expensive.”

The US: A Precursor for the UK?

“The last five years' roadmap in the US is a really good precursor for the UK, and how the UK data breach landscape will develop, how changes in regulation and consumer attitudes will drive a greater focus on the response. Looking at the US can give you a good idea of how things are going to develop. Then it's about how you take advantage of that foresight.”

Michael Bruemmer VP, Consumer Protection at Experian Consumer Services US

Looking at the US today, we can see that :

- The risk of data breach is higher: 46% of US firms have suffered a data breach in the last two years, compared with 17% in the UK;
- Costs are higher: The average US data breach costs £132 per record compared with £104 in the UK;
- Lost business costs are higher in the US, reaching £2.2 million on average, compared with less than £1 million in the UK.

	
46% Risk of breach	17% Risk of breach
£132 Average costs	£104 Average costs
£2.2 million Lost business costs	£1 million Lost business costs

In short, if the UK should follow a similar upward pattern to that which has been observed in the US over the last five years, we can expect to see the incidence of breach rise, and the consequences become substantially more severe.

Businesses erring on the side of caution will be concerned about the compulsory notification, more significant fines and greater public awareness that will be a consequence of the EU Data Protection Regulation – all of which widen the net for the potential for more significant reputational impact and an expanded halo effect of financial damage.

“I do think the UK is taking breach, particularly from a privacy standpoint, very seriously, and I do expect that, when the EU passes its new legislation, it will be like the US when legislation became more stringent - you'll see big changes in the reaction of businesses.”

Michael Bruemmer, VP, Consumer Protection at Experian Consumer Services, US

Best practice 2015: The Customer First Data Breach Response

It is clear that UK organisations still have a lot to learn about planning and delivering an effective data breach response. Moreover, learning those lessons will be vital to minimising the damage caused by data breaches - by limiting the amplifying effect of negative customer perceptions on the overall financial halo effect.

The organisations most equipped to withstand the impacts of data breaches in an ever more demanding environment will take a proactive, integrated approach. They will develop detailed response plans that:

- Focus first and foremost on managing the impact on those affected – recognising that this is where all other impacts ultimately flow from – and let this focus guide communication with the wider public, the media and regulators;
- Identify response teams, roles, responsibilities and lines of communication and draw support and direct involvement at the highest level of the business;
- Identify and put in place master agreements with specialist suppliers – outside legal counsel, insurance, digital forensics, customer support, credit monitoring, and crisis communications;
- Incorporate specific plans for each discipline with the response ecosystem – a digital forensics response plan, a crisis communications plan, a consumer outreach plan, and so on;
- Mandate regular testing and scenario planning to ensure plans are relevant and cover all possible outcomes.

Where we're heading: The expert view - key considerations across the data breach response ecosystem



Customer Support: Protect Customer Relationships Jim Steven, Head of Data Breach Services, Experian

The research behind this paper tells an interesting story about UK businesses' priorities following a data breach. They are clearly concerned about regulatory action, financial consequences and the impact on reputation and customer loyalty - but do not yet understand that managing the impact on affected customers is the key to mitigating all these issues.

Prepare: In a live breach scenario, there are no second chances and a fumbled customer support programme can have disastrous consequences. A clear plan designed to reflect the full range of breach scenarios, and regularly tested, is an absolute must.

- **Respond:** Moving to contact and reassure customers as quickly as possible is vital to containing negative perceptions – demonstrating a clear focus on supporting those affected plays an important role in mitigating wider reputational damage and shaping the regulatory consequences of a breach.
- **Reassure:** The first contact with affected customers sets the tone. It must be clear and concise, reassuring them that the business is taking active steps to address the situation, detailing the support available and giving clear guidance on any immediate action customers should take.
- **Recover:** Giving customers a sense of control following a breach is vital, and that means providing them with simple, easy-to-use tools and support they can use to defend against mis-use of their personal data – from credit monitoring and identity theft protection services to dedicated support helplines.



Insurance: Look Beyond Liability Paul Bantick, UK TMB Focus Group Leader & Underwriter, Beazley plc

There are two elements to cyber and breach insurance. There is the response and the liability, and the response element is going to get much more important. It is much more about the proactive – a solution that draws together all the expertise required to minimise the impacts of a breach.

- **Understand what a 'good breach' looks like:** The characteristics of a good breach are that, at the end of the day, the regulator and the press are saying "Yes, you had a breach, but the response was excellent and has really focused on protecting those affected."
- **Demand for insurance will grow quickly:** In the U.S., the market for breach insurance is already pretty mature. We are at the stage (in the U.S.) where SMEs are buying cover. In the UK it is still early days and, in the main, only the very biggest firms are insuring.
- **Readymade response:** Businesses that do insure want an insurance solution that takes the lead in terms of co-ordinating implementation of a data breach response plan, drawing on a readymade suite of expert vendors to manage the entire process and minimise the damage.
- **Risk management:** The other emerging area of demand over the last 18 months has been pre-breach risk management. We increasingly get involved in helping businesses to develop and test incident response plans.



Legal Counsel: Navigate the Complexity

Margaret Tofalides, Partner and Head of UK and EU Data and Cyber Security Practice, Clyde & Co LLP

Having access to specialist legal counsel is important now and will be vital in future. The speed and quality of the response is going to be ever more important to damage limitation, in terms of the regulators and in terms of public perception - and the ability to draw on specialist legal expertise will be central to that.

- **Build relationships:** It is advisable to have a relationship with the ICO prior to any breach; to know who the right people are to be in contact with, what information you will need to provide and what will be expected of you in the event of an incident.
- **Escalate the issue:** I think it is inevitable that business will have to make cyber security, data compliance and breach response planning board level issues. These are issues that will become as routine for boards of directors as the annual audit, particularly as regulation gets tougher.
- **Notification will be compulsory:** Compulsory notification for everyone will be a game changer. It will significantly increase the potential for reputational damage and the financial impacts that flow from it.



Digital Forensics: Secure the Evidence

Nick Prescott, Information Security Manager,
Blackthorn Technologies

In essence, digital forensics' role in the process is in gathering and interpreting the evidence that could be presented in court, or to a regulator. It provides the definitive account of what happened, how and why – and what needs to be done to prevent a repeat.

Act quickly: There has to be a focus on preserving evidence. Things are improving, but all too often we will get called in when it is almost too late - when preserving the evidence has come in second place amidst the pressure of trying to deal with the live event.

- **Highest standard of proof:** The aim should always be to enable a forensic investigation that delivers the highest standard of evidence – evidence that would stand up in a court of law should that be required.
- **Law enforcement:** There is always the potential that a data breach is the result of criminal activity. One of the first questions we will ask once we get involved is whether the client has informed law enforcement.

Deal with the issues: Forensics plays a vital role in helping organisations to lower risk, by giving them the insight and guidance they need to deal with the vulnerabilities that were at the root cause of a breach.



Crisis Communications: Care, Concern, Commitment

Claire Snowdon, Director, Register Larkin

The big challenge for communications is to be at the table when the senior leadership team is looking at data breach risks and working out what the right response should be. There is still more to do in terms of understanding how well planned communications can help to manage reputational risks.

- **Be prepared for anything:** One of the key things is to scenario plan for every eventuality. In the age of social media and 24 hour rolling news, there is a very good chance that the public and the media will know about a data breach before the business does.
- **Manage the reaction:** In the minutes and hours immediately after the news breaks, it is possible you won't have all the facts. You won't know exactly what has happened, to whom, how or why. The key here is to express care and concern for customers first and foremost, and to communicate control over the situation.
- **Move quickly:** The organisation will sometimes be dealing with criminal activity, so there may be restrictions in terms of what can be said and when, but it is clearly not helpful to wait 24, 48 hours before saying anything. That creates an information vacuum that will be filled by commentators who are unlikely to say things helpful to your cause.

Conclusion

There is no escaping the fact that the UK data breach landscape is going to change rapidly over the next two years. The frequency of breach incidents will continue to rise and tougher regulation, driven by the EU Data Protection Regulation, will raise the stakes significantly.

Fines of up to 5% of global revenues will focus minds in boardrooms across the UK on prevention, but compulsory notification of all breaches will be just as important. Increased media attention, negative reporting and detrimental social media trending around breaches will change public perceptions and behaviour – amplifying and extending reputational damage beyond those affected and driving potentially severe and long-lasting financial impacts from increased customer churn and negative brand associations.

All this will set data breach response planning into sharp focus – and it is clear from our research that all too many UK businesses are simply not doing enough to prepare for the worst. Quite simply, an ‘it’ll never happen to us’ mentality prevails and this is reflected in businesses’ confused views about preparedness: On the one hand they are confident of their readiness, on the other there is a real lack of legitimate planning and preparation and a woeful lack of focus on managing the impact on customers.

The truth is that UK businesses are a long way from ready to deal with the current data breach landscape, let alone the high octane environment we are likely to see emerge over the next two years. The time to prepare is now and that must start with a realisation that the customer is the starting point.

The customer must be the number one priority in breach response planning, because the financial and reputational consequences of a data breach flow from its impact on customers, and from the business’ effectiveness in managing those impacts.

As a result, the customer response must be embedded through the overall response, not an afterthought. A focus on customer response, reassurance and recovery must drive every aspect of the overall breach response – it must sit at the heart of a comprehensive response plan and act as a vital guiding principle for legal, forensic and crisis communications activity.

In short, the next two years will see the emergence of the ‘Customer First Data Breach Response’.

About Beazley

Beazley is unique among insurers in having a dedicated business unit, BBR Services, which focuses exclusively on helping clients manage data breaches successfully.

About Blackthorn Technologies

Blackthorn Technologies is recognised as a pioneer in providing digital forensics and governance, risk and compliance services and solutions, working across the public and private sectors.

About Clyde & Co LLP

Clyde & Co is a leading international law firm with over 300 partners and 2,500 staff based in 40 offices cross 6 continents. Clyde & Co is unique in focus, scale and reach and our work is cross-border, high profile and complex.

Regester Larkin

Regester Larkin is a specialist international consultancy that works with organisations facing – or preparing to face – challenges or crises.

Experian

Experian is the leading global information services company, providing data and analytical tools to clients around the world. Experian has first-class technology and expertise in identity protection and verification, fraud prevention and data breach resolution, helping organisations grow and sustain successful relationships with their customers.

Research Methodology

On behalf of Experian, ComRes interviewed 400 medium and large UK businesses online between the 22nd December 2014 and 3rd January 2015. All respondents were screened and had involvement or knowledge of their company’s data breach policy.

ComRes also interviewed 2,056 GB adults online between the 9th and 11th January 2015. Data were weighted to be representative of all GB adults aged 18+.

Registered office address: The Sir John Peace Building, Experian Way, NG2 Business Park, Nottingham, NG80 1ZZ, United Kingdom
www.experian.co.uk/databreach

Experian Ltd is authorised and regulated by the Financial Conduct Authority. Experian Ltd is registered in England and Wales under company registration number 653331.

© Experian 2015.

The word "EXPERIAN" and the graphical device are trade marks of Experian and/or its associated companies and may be registered in the EU, USA and other countries. The graphical device is a registered Community design in the EU.
All rights reserved.