

Data Breach: Supply Chain Risk

Taking control of risk and vulnerabilities

February 2018



Contents

FOREWORD:	01
Data Breaches & Supply Chain: Our new insight	
INTRODUCTION	02
RESPONSIBILITY:	03
Who is ultimately responsible - you or them?	
THIRD-PARTY RELATIONSHIPS:	06
Where is your data?	
CUSTOMER CONUNDRUM:	08
What is at stake? Quick reference checklist	
CONCLUSION:	10
Moving the security mindset on	
ABOUT EXPERIAN'S DATA BREACH RESPONSE SERVICES	12



Jim Steven
Head of Data Breach
Response, Experian

Foreword

Taking control of risk within your supply chain

In the past year alone, we've seen a wave of cybercrime and data breaches across the world. In Britain, businesses and organisations have been left unable to carry out routine business services as a result of these attacks. The UK National Cybersecurity Centre has warned that it expects a 'category one' attack (the most serious tier, needing a national government response) within the near future.

It's part of everyday life, individuals and businesses use websites, social media pages, cloud services and there is no doubt that there is a surge in new sophisticated technological intelligence. This is weaving a new web of complexity when it comes to managing, transferring and utilising rich data insight – all in the endeavour to serve customers with relevant, real-time services and positive experiences in life events.

Linked to this is the increasingly complex operating model businesses sometimes need in place, resulting in a reliance on 3rd parties. The sophisticated networks of supply chains means the potential business risks increase, but so do the exciting opportunities to deliver more for customers. It is a conundrum every business faces.

About the research

Experian has commissioned our trusted partner, the leading research consultancy ComRes, to unearth new insights into the topic of data breaches and third-party suppliers. ComRes is a member of the British Polling Council.

On our behalf, ComRes surveyed 2,033 British adults aged 18+ online between 8th - 9th November 2017, and 202 decision-makers in information security and data breach management in Great Britain online between 23rd October and 1st November 2017. Quotas were applied to the sample in order to achieve broad representativeness of the sample, achieving 51 medium-small businesses (50-99), 51 medium-large businesses (100-249) and 100 large businesses (250+).

Introduction

The purpose of this whitepaper - Supply chain risk exposure

A broken link involving just one of your suppliers can send security concerns down your entire chain. The purpose of this whitepaper is to understand and reveal more about the relationship between organisations and third-party suppliers when it comes to cybersecurity. It also looks at data breach risk and response, and the impact on and views of consumers.

EU General Data Protection Regulation (GDPR) is nearing

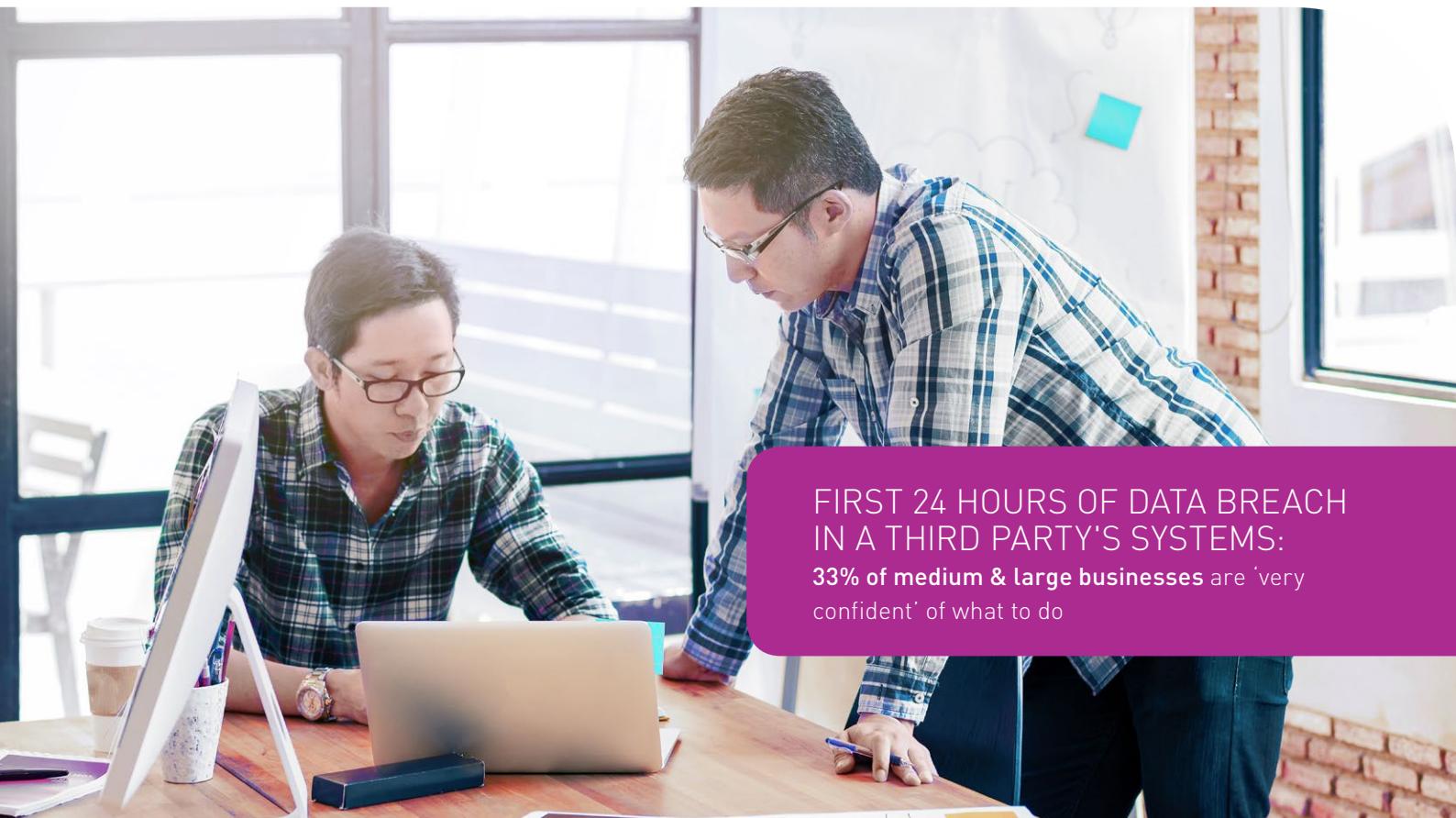
Organisations are still grappling with GDPR readiness. On 25th May 2018 the GDPR will come into force and all organisations processing personal data will be required to comply with it. There is potential for more requests from customers asking businesses to prove that they are GDPR compliant. That means that you will need to ensure that you are compliant and have the confidence that your supply chains are compliant too.

[Read more in our whitepaper...](#)

Responsibility: When it comes to cyber security, who's in charge – you or your supplier? And when a data breach happens, who's in charge?

Third-party relationships: Do you really know where your suppliers hold your customer data? How secure is it? And are they GDPR compliant?

Customer conundrum: Customers are placing a lot of trust in organisations when it comes to their data. Is that trust protected by rigorous checks in your supply chain, or is your reputation at stake?



FIRST 24 HOURS OF DATA BREACH IN A THIRD PARTY'S SYSTEMS:

33% of medium & large businesses are 'very confident' of what to do

RESPONSIBILITY: Who is ultimately responsible - you or them?

Moving beyond your own plans to your third parties

Businesses are improving their data breach resilience, year on year. 91% of medium and large businesses in the UK now have data breach response plans in place. However, while companies tackle securing their own networks, software and data, the question around assessing suppliers and partners within these plans is still an integral piece of the perfect puzzle.

The businesses we surveyed have identified four of the highest risks facing them as a result of using third-party suppliers: loss of personal data; online fraud; identity fraud and financial loss or damage.

HIGHEST RISKS OF USING 3RD PARTY SUPPLIERS

- Loss of personal data
- Online fraud
- Identity theft
- Financial loss or damage

Business resilience

Data breaches appearing via third parties are a growing problem across many industries and sectors. And they can be hard to defend against. Loss of customer or employee personal data is clearly the biggest worry for organisations using third-parties. With a reduced ability to control the environment, supply chain security is clearly not as stringent as many businesses would like it to be.

Is your business vulnerable?

Cyber criminals are resourceful and resilient and move quickly with the moment. Any business is vulnerable to a data breach, although the readiness of response plans will greatly determine the potential outcome and risk of reputational damage.

As your supply chains become more complex, your exposure naturally increases – and that's unavoidable. Hackers will seek out to find ways to access and retrieve sensitive data, which can have a domino effect on the rest of the supply chain network. This results in periods of tension and detriment to business services.

Third-party suppliers can be a cyber security blind-spot for many organisations. Being aware and having regular updates will support your efforts to protect from potential risks in the future.



Data breach: Supply chain risk

Smaller businesses take note

Encouragingly, 92% of medium and large businesses review the policies and procedures of their third-party suppliers who they currently work with at least once a year. And while this is a positive step, from our experience at the data breach frontline, just once a year has the potential to increase risk. Business change over a year just from a technological perspective continues to evolve at astonishing rates as do the people on the ground.

Is there a correlation between size of business and risk?

There is a definite correlation between the size of business and security risk. While 43% of large businesses review third-party policies and procedures quarterly, only 20% of medium-small businesses do. Understandably, this can be down to smaller budgets and resources. We believe there is much to be gained by focussing on this element as the costs of a data breach on an SME could severely impact the ability to trade. Taking the right steps can certainly help ensure that the earned positive reputation can be maintained.



Who's accountable in the aftermath?

This is perhaps the most intriguing question of all when it comes to third party relationships and data breaches. More than half of businesses say both the organisation and the supplier are equally accountable in the event of a data breach within a third-party system. Interestingly, of those who have experienced a data breach of any size in the past two years, a quarter say that the third-party supplier would be accountable for the management of the response, if the data breach had happened within the supplier's system, compared to 13% of those who have not experienced a data breach.

Would you really hand over the responsibility?

While this is what businesses have said, in reality, would this really happen? When your entire reputation is at stake, would you put your trust in another to break the news to your customers – in the correct legal way and in the compliant timeframe? All this would be while your supplier is challenged internally with the other devastating ripple effects of the breach. This has the potential to increase the risk of reputational damage and leave the organisation vulnerable and without the ability to control and manage the situation effectively.

Our research found that businesses review policies & procedures of 3rd party suppliers quarterly:

43%

Large businesses

20%

Medium-small businesses

Bigger picture approach

A change in mindset may be wise, and taking a 'bigger picture' approach can really help reduce the risk. Any third-party supplier you work with, large or small, local or overseas, has the potential to make your business vulnerable. Information security is therefore no longer an internal task. It must be accounted for up and down the supply chain. Businesses need to collaborate and have coordinated security systems across the board, rather than disparate programmes that could expose everyone involved.

Taking the vital steps to a stronger supply chain network

Security is only as strong as the weakest link. Introducing supply chain risk management processes throughout your entire corporate structure is a vital first step. And it needs to start at the top. C-suite and the Board need to establish their strategy for cyber risk management first and foremost. Given the potential damage of a data breach, it is no longer plausible for the IT department to be entirely responsible for an organisation's cyber security, let alone that of third

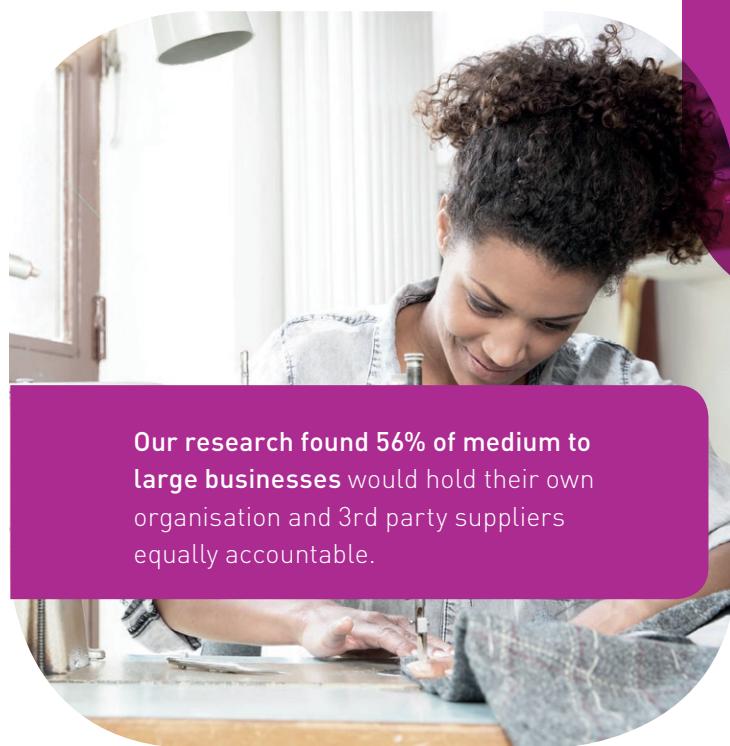
parties. Greater collaboration across key functions is a positive step, and leading this throughout the supply chain will bring all parties together to create a united view on the situation.

It's exciting and fast moving, but fair to say supplier management is no easy task for organisations. The constant enhancements in technology and service needs puts any procurement environment on a demanding schedule. Balancing the need to innovate, whilst weighing up the potential risks has never been more important.

25%

of businesses who have experienced a breach recently believe the 3rd party supplier would be accountable for data breach response compared to 13% of those who have not experienced a data breach.

Our research found 56% of medium to large businesses would hold their own organisation and 3rd party suppliers equally accountable.



THIRD-PARTY RELATIONSHIPS: Where is your data stored?

How well do you know each other?

First and foremost, do you know where your – and therefore your customers' – data is? How is data processed and are appropriate technical and organisational measures in place to protect it? And do they have strong IT protocols? These vital questions need to be answered before you go into partnership with a third party, and monitored regularly afterwards.

25% of businesses don't think or don't know if their 3rd party suppliers could notify them within 72 hours of a data breach.

Being in control, not in the hands of your supplier?

It matters now more than ever because GDPR is just around the corner. If you're GDPR compliant yourself, but are not totally sure about your supplier's data storage, you may be in breach – and face costly sanctions. The fact that our new investigation into this matter has revealed that 25% of businesses don't think or don't know if their third party suppliers could notify them within 72 hours of a breach is of concern. That means a large number of businesses of all sizes have no control. They are entirely in the hands of their suppliers, who may not be in a position to share something as serious as a breach that's exposing your customers' personal information – whether intentionally or not. Essentially, someone else is in control of your destiny as a business.

GDPR: data breaches and reporting within

72 hours

GDPR: a reminder – it extends into your supplier network

The Information Commissioner's Office is responsible for regulating and enforcing compliance with GDPR in the UK. At the heart of the new law is greater transparency and accountability. Under GDPR, it will be mandatory for a data controller to report a personal breach unless it is unlikely to result in a risk to people's rights and freedoms. The ICO is recommending that in the run-up to May 2018 "you should make sure you have the right procedures in place to detect, report and investigate a personal data breach." Personal data breaches must be reported, without undue delay and, where feasible, no later than 72 hours after becoming aware. Failure to report a breach in line with the requirements could lead to enforcement action and possibly a fine. If a third-party supplier suffers a personal data breach involving personal data your organisation is data controller of, and does not inform you of the incident promptly, then they're putting you at risk of contravening GDPR. As you read this, you're very likely to have put the right plans in place internally. But have you thought of how GDPR extends through your vendor network?



How do you audit to make sure your suppliers are keeping you within the law?

Supply chain and customer data quality checks

Auditing is just part of supply chain hygiene. We believe you need to take control and make sure exposure is limited, rather than leaving it to your suppliers. Too many businesses will be in a weak position when GDPR comes into play. The statistics in our findings also show that high numbers of customers may not know their data has been compromised. This is linked to the fact that businesses are holding contact information which is inaccurate and not up to date and so the individual may never receive the notification. Businesses can quickly remedy this with frequent data quality checks with little effort and maintain this when incorporated into business as usual processes.

Insider threat - Do you know the individuals on the ground?

While acts of negligence or simple human error are often likely to be the root cause of a data breach, the insider threat can increase as more third-party vendors work with an organisation. As we've seen with data checks when it comes to supplier reviews, our findings also show that security auditing is an area that can be quickly cured of increased risk.

Data quality checks can support your efforts towards being compliant:

37% medium-small business, 49% medium-large and 56% large businesses plan to carry out data quality checks with 3rd party suppliers.

Vetting people – your extended team...

Carrying out regular background checks on staff and contractors can put the organisation on the front foot – keeping customers and employees safe. When we asked organisations if they carry out vetting of key individuals within third-party suppliers as part of the relationship they have with them, the results were interesting. Overall, 60% say they do this for all 3rd party suppliers. But what about the remaining 40%? What's more, only 29% of businesses who carry this out do so quarterly.

Businesses and auditing:

49% businesses carry out security audit questions

36% penetration server testing

33% carry out site visits

SECURITY AUDITING – How many businesses do it?

In our view, the auditing process needs to be frequent and extend right through the entire organisation. To withstand a data breach, companies must know the intricacies of their own networks – what data suppliers hold, where it is stored, and significantly, who exactly has access to it. When the economic benefit of using a third-party vendor comes at a compliance cost. The standard of compliance needs to be yours, not theirs.

TOP 5 TIPS FOR ONBOARDING SUPPLIERS

- Diligent background checks and screenings of individuals
- Verify security practices and procedures of vendors, suppliers and partners
- Document and agree governance criteria and check point timings
- Limit access to data in all your networks to those that only need access
- Data cleanse & quality check frequently

CUSTOMER CONUNDRUM: What's at stake?

Always make the customer the priority

While we are discussing the most important consideration of data breaches last, of course, your customers will be your top priority. Your customers will rely on you providing details of the incident and will be upset and concerned. Doing all you can at this point to reassure and guide will support your efforts in keeping a trusted, ongoing relationship in the future.

Third party security is your responsibility

As we mentioned at the start of this whitepaper, more than half of businesses believe that they are equally accountable if a data breach happens in the third-party system. And yet, nearly half of consumers (48%) say they would stop using the company following loss or theft of personal details. Again, this backs up our view that third-party security needs to be your responsibility. In our experience, consumers rarely make any distinction between you and your vendors.

Trusting relationship

Our data shows that consumers are placing a lot of trust in brands. 56%¹ of the general public feel comfortable sharing general data with a company. While 29%¹ happily hand over personal, identifiable information. That faith needs to be protected. But can you be completely confident that trust is being reciprocated when it comes to your supplier network? Can you be certain that your consumer data is being treated with respect, and is not at risk of exposure anywhere down your supply chain?

51% of consumers expect financial compensation if their information is lost or stolen

Crisis management – vital questions your customers will be looking to you to answer

As we all know, how a crisis is handled can save or severely hamper a brand's reputation. Customers expect a lot from an organisation when things go wrong. For example, most customers expect advice and support on what to do in the event of a breach. They also expect those responsible to be pursued, and about half will seek financial compensation. Are you able to fulfil these demands in the event of an emergency?

If the breach has taken place somewhere in your supply chain, will the financial compensation come from you, or your vendor? And who will pursue those responsible? These are all vital questions that need to be addressed with your supplier when you enter an agreement.



65% of consumers expect advice and support on what to do after a breach

¹Censuswide data, commissioned by Experian November 2017, sample of 2,000 UK consumers

Contacting your customers

As an aside – but interesting – note, our investigation has exposed controversy about the way you should contact your customers to alert them to a breach. While the majority of people would expect to be notified by email (66%) or to a lesser extent by telephone (46%), in our experience, both these methods has the potential to play into the hands of fraudsters.

Notifying an individual of the loss of their personal information is an important and sensitive message. Delivering a physical letter with vital information to each and every individual, clearly positions the importance the organisation places on the situation.

We would recommend you have a fully documented plan along with pre-prepared template communications, which are approved and ready to go. The key question is - Are your suppliers completing the same preparation?



CONCLUSION: Moving the security mindset on

Businesses need to have an 'at risk' mindset

While many companies today are on top of common data security issues, no set of measures is completely infallible to a breach. And when you throw complicated networks of suppliers into the mix, this is when business security can start to unravel.

Supply chain attacks pose a serious threat to all organisations. The biggest vulnerability that this whitepaper has revealed is that too many businesses do not know where their suppliers are keeping their data, and who has access to it.

As GDPR becomes a reality, the whole landscape for UK businesses is changing dramatically. We speak to many organisations daily, and many are working towards becoming compliant. However, when it comes to extensive supply chains, our latest investigation has shown that there are big considerations for businesses.

We understand that relationships with third-parties are complex and challenging. However, simple tick-box exercises will not safeguard the business when it comes to securing the supply chain, and therefore your customers' personal data. If just one of your vendors' security is weak, your entire business resilience is jeopardised. We believe a significant mindset shift needs to happen in the future, to one that's 'at-risk' at all times.



“Organisations we work with are still surprised about just how complex it can be to notify customers. This is further compounded when the supply chain is complex and it is a 3rd party who has suffered a breach. Getting ready in advance, agreeing who is in control, is the only sure way of ensuring a response reaches those affected and in good time.”

Jim Steven, Head of Data Breach Response, Experian



About Experian's Data Breach Response Services

We help organisations to prepare and respond in the event of a data breach – including your third-party supplier.

We understand your primary concern at the time of a data breach incident will be the people affected. Having the ability to notify, provide reassurance and offer remediation at this critical time will help you to maintain trust, reduce reputational impact or financial loss.

Immediate or pre-readiness response assistance:

We have more than 10 years' experience supporting thousands of organisations of all sizes to respond, reassure, and recover in the event where personally identifiable information has become compromised.

When you need immediate assistance to support a live incident we are here to help you. Or we can work with you proactively to put a pre-breach readiness plan in place, ensuring you are prepared for the future with increased confidence.

Do you have a question?

If you have any questions relating to this whitepaper or Experian's Data Breach Response services the team are always here to answer your questions in complete confidence.



Jim Steven
Head of Data Breach Response

Experian Affinity Partnerships
jim.steven@experian.com
+44 7972 298698

Email: breachresponse@experian.com
www.experian.co.uk/databreach
Call us on 0844 4815 888
Outside UK +44 844 4815 888



Sarah Longstaff
Senior Marketing Manager

Experian Affinity Partnerships
sarah.longstaff@uk.experian.com
+44 7967 567014

Other helpful resources:
Data Breach Response step by step guide (2017)
Readiness vs Reality whitepaper (2017)
SMEs Under Threat whitepaper (2016)
Data Breach Whitepaper 2.0: Data Breach Readiness (2015)
www.experian.co.uk/databreach





Registered office address:
The Sir John Peace Building, Experian Way,
NG2 Business Park, Nottingham, NG80 1ZZ

www.experian.co.uk/databreach

© Experian 2018.

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

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.

Legal Notice: The information obtained herein is not, nor intended to be, legal advice. We try to provide quality information but make no claims, promises or guarantees about the accuracy, completeness or adequacy of information contained. As legal advice must be tailored to the specific circumstances of each case and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent legal counsel.