FTI CONSULTING

THE ANATOMY OF A CRISIS Volume 3

WHEN NOT IF

What can cyber breaches of the past 10 years teach us about how to prepare for them in the future?

2020

Introduction

Our research tells us that a cyber breach is the top concern for boards and management teams. They prioritise it over technological disruption concerns, product defects and even trade restrictions and they report lost revenue, customers and employees among the consequences. And yet we see that fewer than half of those business leaders are preparing to manage their cyber risk proactively in the year ahead. We believe that this paradox is worth investigating. In the third volume of *The Anatomy of a Crisis*, we aim to investigate the cyber landscape in more detail.

Our objective with this report is to provide an overview of the cyber breach landscape, the impact of these breaches and how companies have responded. What worked well and what didn't work? We hope to provide critical information to clients for the moment they face cyber breaches of their own.

About The Anatomy of a Crisis series

In this age of round-the-clock company scrutiny, we see almost as much focus given to how a company handles a crisis as the crisis itself. With turbulence in our world growing on a daily basis, and the always-on nature of the news, crisis has become a daily consideration for business. If handled poorly, crises can cause deep and long-lasting damage to a company's reputation. If handled well, a crisis can become an opportunity for a company's management team to demonstrate their mettle to investors, customers and employees.

With this in mind, FTI Consulting is undertaking a series of research studies into crisis events, called *The Anatomy of a Crisis*. Our aim is to shine a light on those crises and assess how they played out with a view to helping businesses successfully navigate future disruptive events of their own. Historical context and – crucially – data can be the critical factors in helping management teams make the right decisions in the heat of a crisis moment.

Through our research and in-depth analysis, FTI Consulting will help management and communications teams support their instincts with empirical data when considering their organisation's cyber breach response strategies and plans.

About this report

We used two different sources to compile the data for our report. The first is an analysis of 300 publicly-available cyber breaches over the past 10 years, including details on the type of breach, company performance, impact, company response, etc.

The second data source is our 2020 Resilience Barometer, which contains interviews with over 2,000 company leaders from G20 countries. References regarding the impact to people and the way they responded come from this study.

Part 1 – Cyber Breaches
Provides an overview of the 300 publicly reported cyber breaches – where they have happened as well as the scale and type of breach.

Part 2 – Breach Impact
Assesses the impact that cyber breaches have had – the financial, operational and reputational damage that they cause.

Part 3 – Company Response
Examines how companies responded – their communications approach and the operational changes they made as a result of the breach.

This analysis will help management and communication teams support their instincts with empirical data when they consider their own cyber breach response strategies and communications plans.

PART 1
CYBER BREACHES

Types of cyber breach

This section provides us with an overview of the cyber breach landscape, looking at 300 cyber breaches from 2009 to 2019. Of course, many more cyber events have occurred, but not all have been reported. This is a list of the largest breaches over the past 10 years across the world – those which have attracted the greatest public attention.

At the moment of a cyber breach, this information will allow management teams to see how serious their own breach is, relative to those that have gone before.

Breaches from inside and out

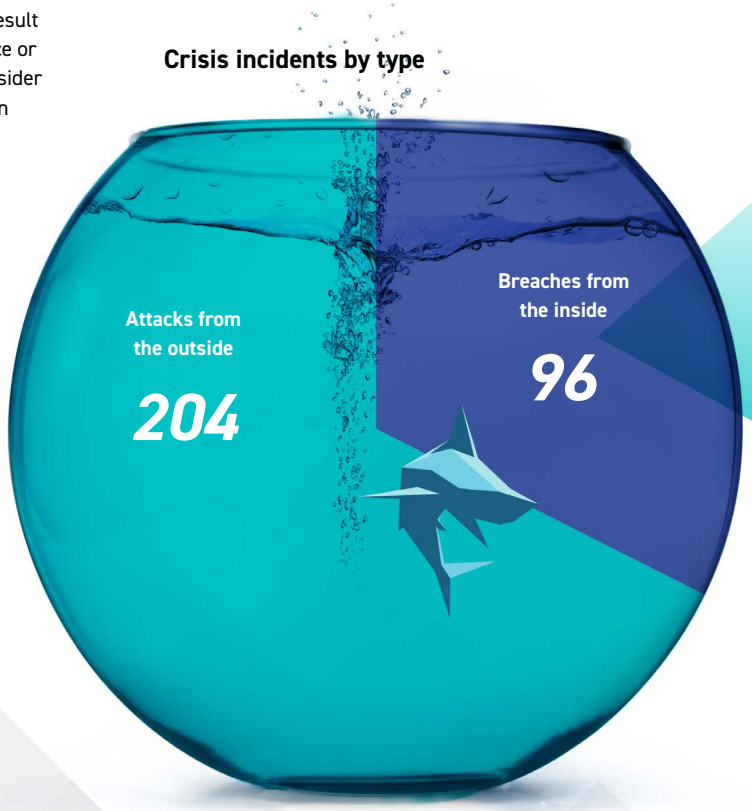
At the moment of cyber breach, the research presented in this study will allow management teams to gauge the severity of their breach relatively to those that have previously occurred.

This first image shows whether breaches have come from outside the organisation – including hacks, denial of service, ransomware and other forms of attack – or whether the incident has arisen as a result of internal issues – such as an employee hack, a misplaced device or poor security. We have cut the data this way as we will later consider whether internal lapses have more significant consequences than attacks from external actors.

More than two thirds of the incidents came from attacks from outside the business. Management teams should prepare for these threats with activities such as cyber vulnerability assessments, penetration testing and threat- hunting operations. This will help better understand your cyber risk profile and ultimately build a robust security posture, which is the best way to prevent a breach from occurring.

The remaining third came from incidents which appear to have originated from inside the business.

We have broken down these 96 incidents into the four buckets mentioned above. The most prevalent cause was internal security lapse, which could have been avoided. Lost hardware, deliberate employee breaches and human errors are also important factors, underlining the need for proper employee training and awareness.



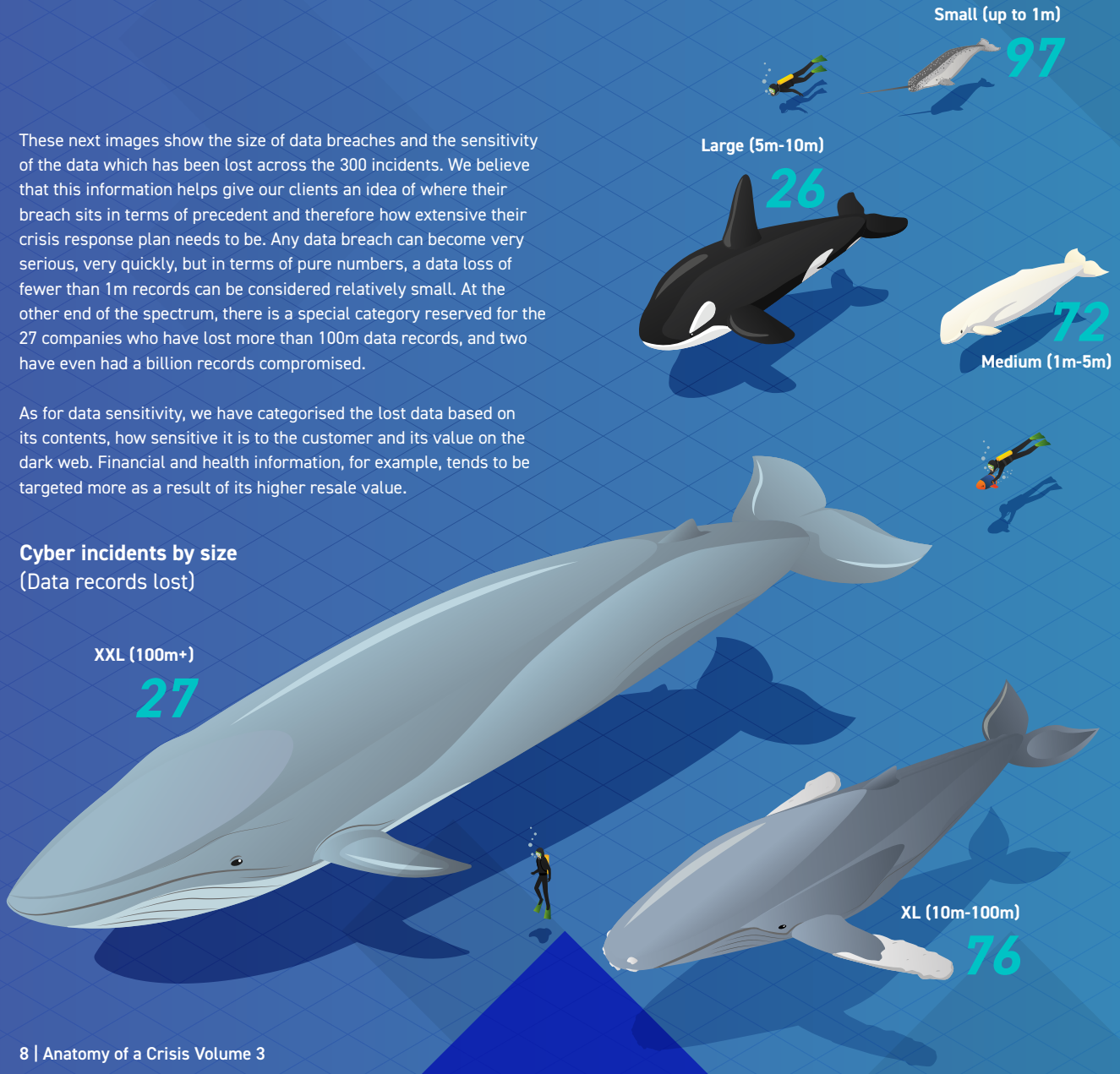

Breaches
from the inside
Hack from inside
the business
12
Internal security lapse
40
Human error
17
Lost laptop,
USB, drive
27

Size and sensitivity of cyber breach

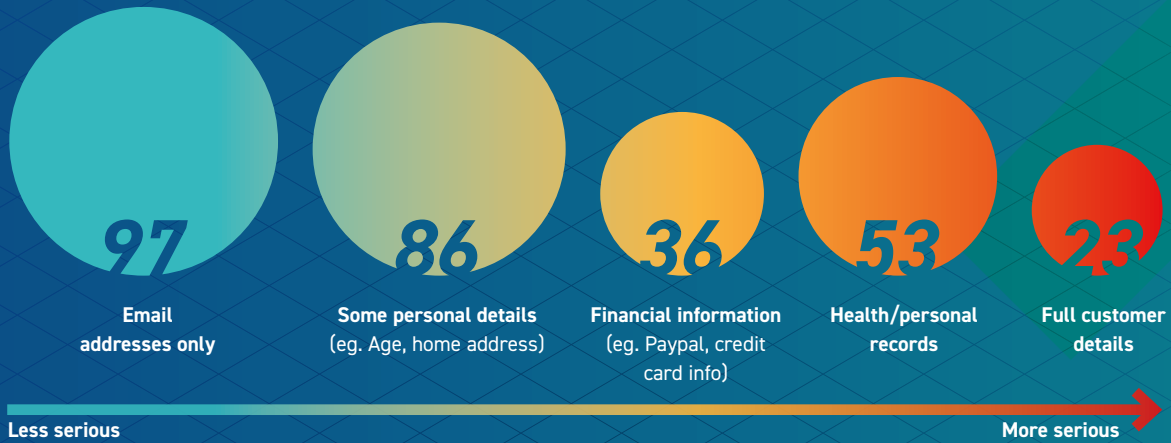
These next images show the size of data breaches and the sensitivity of the data which has been lost across the 300 incidents. We believe that this information helps give our clients an idea of where their breach sits in terms of precedent and therefore how extensive their crisis response plan needs to be. Any data breach can become very serious, very quickly, but in terms of pure numbers, a data loss of fewer than 1m records can be considered relatively small. At the other end of the spectrum, there is a special category reserved for the 27 companies who have lost more than 100m data records, and two have even had a billion records compromised.

As for data sensitivity, we have categorised the lost data based on its contents, how sensitive it is to the customer and its value on the dark web. Financial and health information, for example, tends to be targeted more as a result of its higher resale value.

Cyber incidents by size
(Data records lost)



Cyber incidents by data sensitivity
(Data records lost)



For a management team handling a data breach, these charts provide useful context. For example, a breach of 100,000 records would be small in relation to other historical breaches, but because the data loss contains personal medical information, it is materially more sensitive and likely to have significant repercussions as a result.

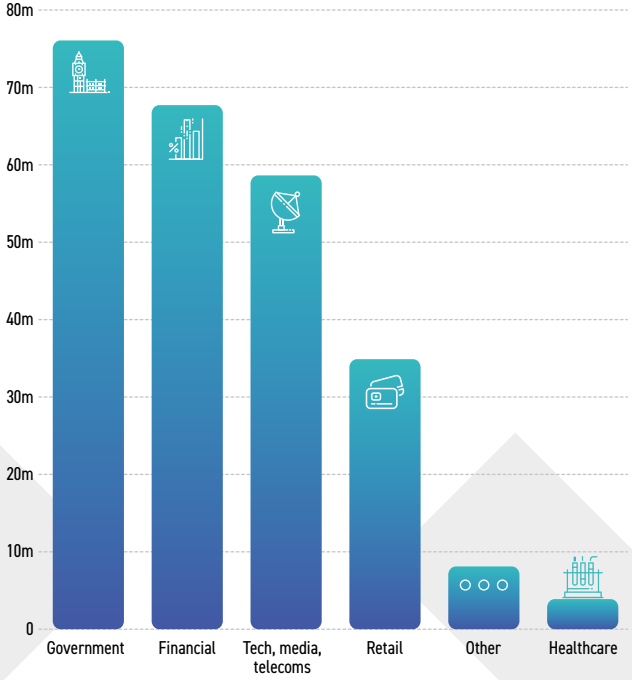
Finally, we looked at cyber incidents by sector. The telecom, media, and technology (TMT) sector dominates as it incorporates so many businesses – telecoms, media, app and web businesses – that are fundamentally digital and therefore susceptible to external technological interference. Healthcare, government and financial organisations are also featured due to the sensitive and valuable data they hold. In 'other', we see critical infrastructure businesses, such as energy and transport, though these are less prevalent than other categories.

Cyber incidents by sector

Types of cyber breach by industry and year

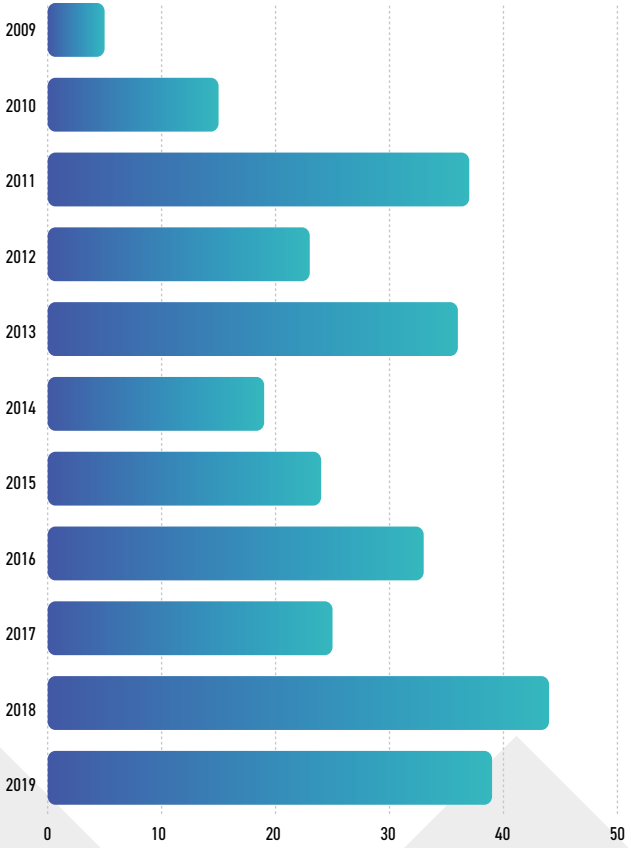
Next, we cut the industry data against the size and sensitivity of the breach. Unsurprisingly, we see that government, financial entities and TMT businesses are on the receiving end of some of the largest attacks. Despite the frequency of hacks on healthcare businesses, the data losses tend to be much smaller, likely due to the comparatively small customer data pools held by hospitals and local health organisations. As more of this sensitive medical data starts to be shared and combined to allow artificial intelligence (AI) to look for patterns in diagnosis and treatment, we can expect greater interest from malicious actors. Security efforts will need to be doubled.

Size of breach by sector



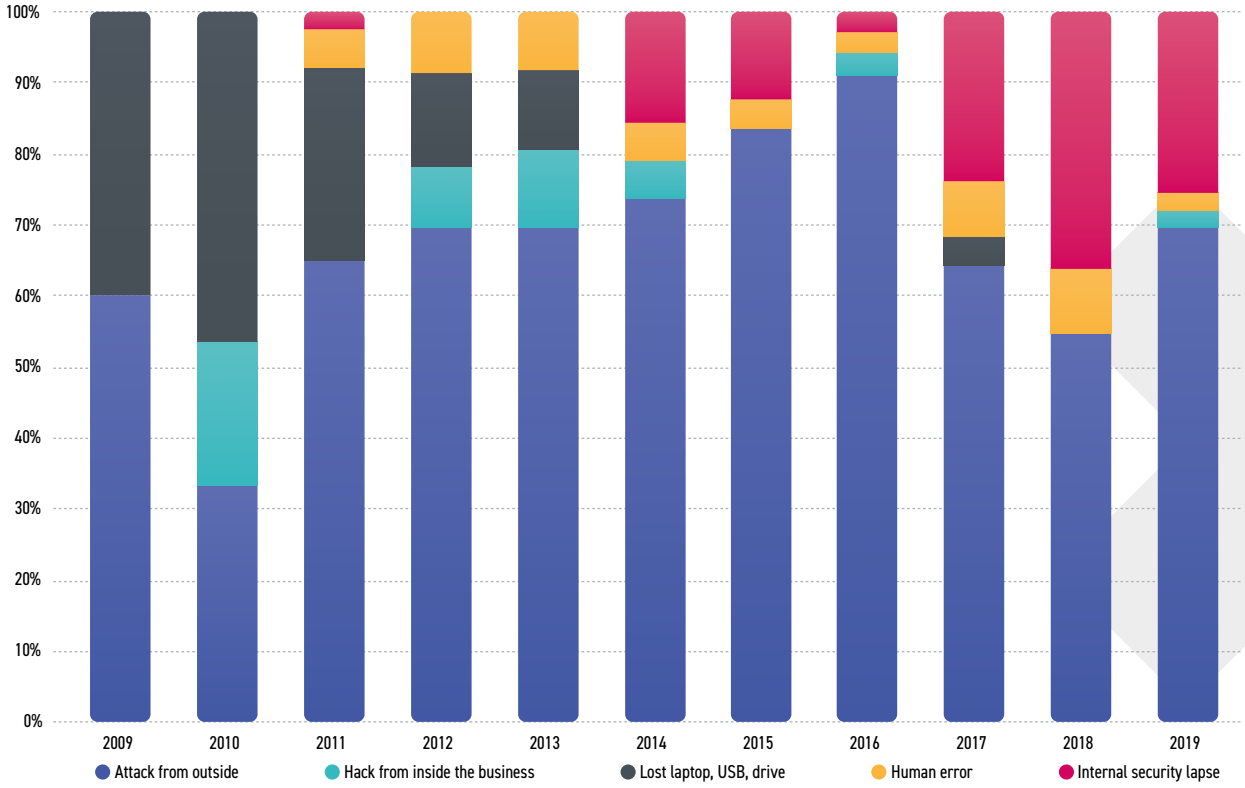
Finally, we were interested to see whether things have changed markedly over the time horizon of our study. As we analyse the last 10 years, we can see that there has been a steady, if not uniform, increase in high-profile cyber breaches over that time.

Cyber incidents – 2009-2019



In terms of the type of breach, we see evidence of internally-caused breaches decreasing in regularity over the period. The incidents where devices have been lost stop altogether from 2013, and we see only a handful of insider hacks after that year. Culture and education efforts inside companies appear to be having the desired effect. However, incidents where breaches have been caused by internal security lapses seem to increase in regularity in the latter part of the decade. Progress may be being made on internal awareness, but avoidable security breaches are gaining in frequency, most notably among web-based and data businesses that have access to large data hordes.

Cyber incidents by type – 2009-2019



The view from business in 2019

In our survey conducted for the Resilience Barometer 2020, we asked business leaders to list the corporate risks they had experienced in the past year. A cyber-attack was the most common risk reported, overshadowing other threats such as product defects, leaks, trade restrictions and litigation.

27% of respondents reported that their business experienced a cyber breach in the past year. This number increases to 33% among those companies where leaders report feeling under extreme pressure to increase revenue, which underlines the truism that governance can sometimes be overlooked in the pursuit of growth at all costs.
We then asked what type of cyber-attacks their business had sustained in 2019. The most common breach was a phishing attack, followed by loss of customer or patient data, followed by the loss of third-party information.

As leaders look to the year ahead, cybersecurity is again the number one concern, and 26% of leaders expect their business to be harmed by an attack in 2020.

CYBER ATTACK #1
corporate risk
expected in 2020

Which of the following cyber attack has your organisation been negatively impacted by over the last 12 months?

PART 2
THE IMPACT

In Part 2, we examine the impact that cyber breaches have had on businesses. This data will provide management teams with a good sense of the operational, financial and reputational damage that can come from cyber issues – useful context as businesses plan their own responses.

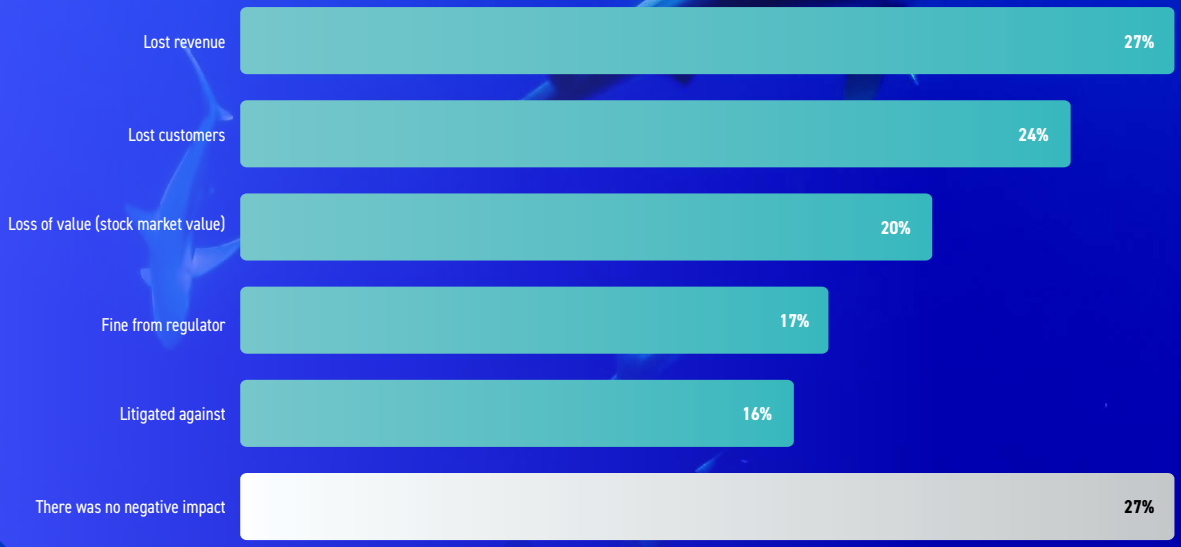
The impact

Financial Impact

We begin with the financial impact, where we see cyber-attacks having a disproportionate effect on business. Of all the corporate risks mentioned, even compared to product defects, trade restrictions or technological disruption, cyber is perceived to have the greatest impact on lost sales.

According to FTI Consulting's 2020 Resilience Barometer, lost revenue is also the number one impact mentioned as a consequence of cyber attacks. 27% of business leaders report lost revenue as a negative impact of a cyber-attack in 2019. Further financial impacts can come from regulatory fines and litigation – 17% and 16% of businesses respectively incurred these impacts.

What was the negative impact as a direct consequence of these cyber-attacks?



Operational impact

The operational impact of a cyber breach can also be significant. The most obvious immediate consequence is data loss. 26% of business leaders say their breach resulted in the loss of customer data, 25% report losing third-party data and 19% say that their business lost intellectual property (IP) because of their breach. It is not surprising, therefore, that 24% of business leaders believe that customers have been lost as a direct result of a cyber-attack, a number which is borne out of the lost revenue statistic previously listed.

The impact of these incidents is also felt internally. 18% of businesses report employees exiting the firm and citing the cyber breach as one of the reasons for leaving. A similar number – 16% – report that potential new hires decided not to join the firm because of the breach.

Another operational consequence of a cyber breach is that attention is diverted from the day-to-day management of the business. 20% of businesses reported this impact. In another of *The Anatomy of a Crisis* study, we report on the human cost of crisis – the mental and physical impact on management and the cost on relationships with colleagues and family.

These impacts start to answer the question – why do management teams care so much about cyber breaches?

26%
Lost customers
due to cyber breach

The impact

Reputational Impact

The final piece of the impact puzzle is the issue of reputation. We used three measurements for reputation - share price, media volume and media sentiment.

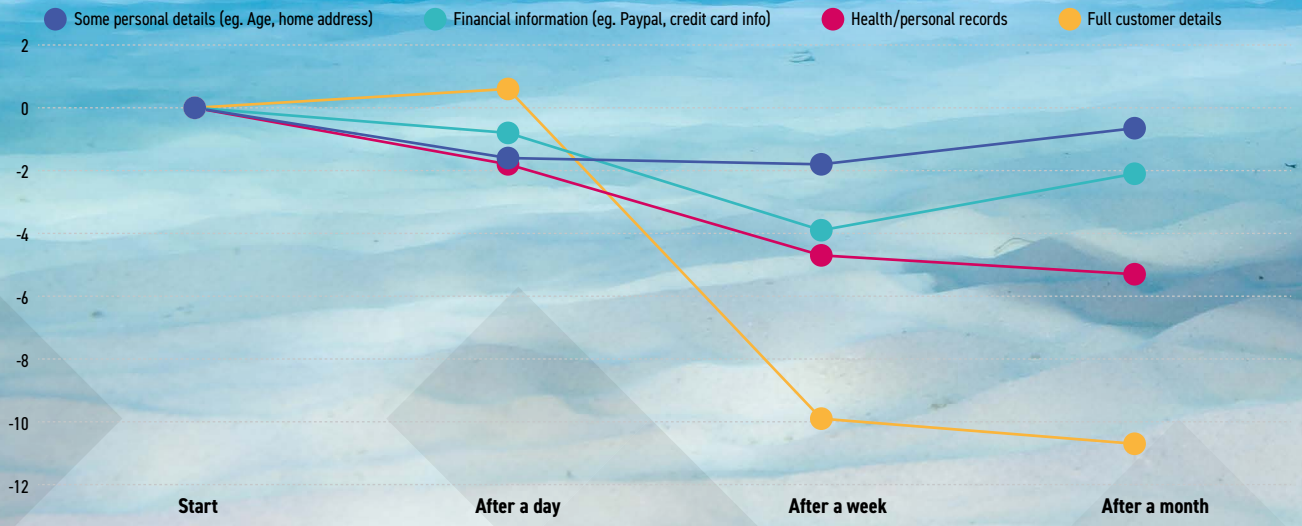
Share price:

In our previous Anatomy of a Crisis reports, we suggested the share price reaction to cyber-attacks tends to be relatively modest compared to other forms of crisis, such as fraud and accidents. Although 20% of business leaders reported share prices dropping, our 2017 survey showed that while we see shares decrease in the first few days after a cyber-attack, within three months, on average, the stock tends to recover.

We have found much of the same with this research. For data breaches that do not contain the most sensitive data, the market reaction tends to be relatively benign. This context is helpful as companies start the process of deciding where to focus communications energies at the announcement of a breach. There is temptation to be 'investor-first' with corporate communications and to be led by the needs of that group. However, the data suggests that the market tends to be forgiving, and given what we have learnt about how customers and employees react to news like this, management may be well advised to focus their attention on these groups first.

The exception to this is where the data lost is of a particularly sensitive nature. Here, the loss of value is significant. So, organisations should pay close attention to the sensitivity of the compromised data when they decide how best to communicate their response.

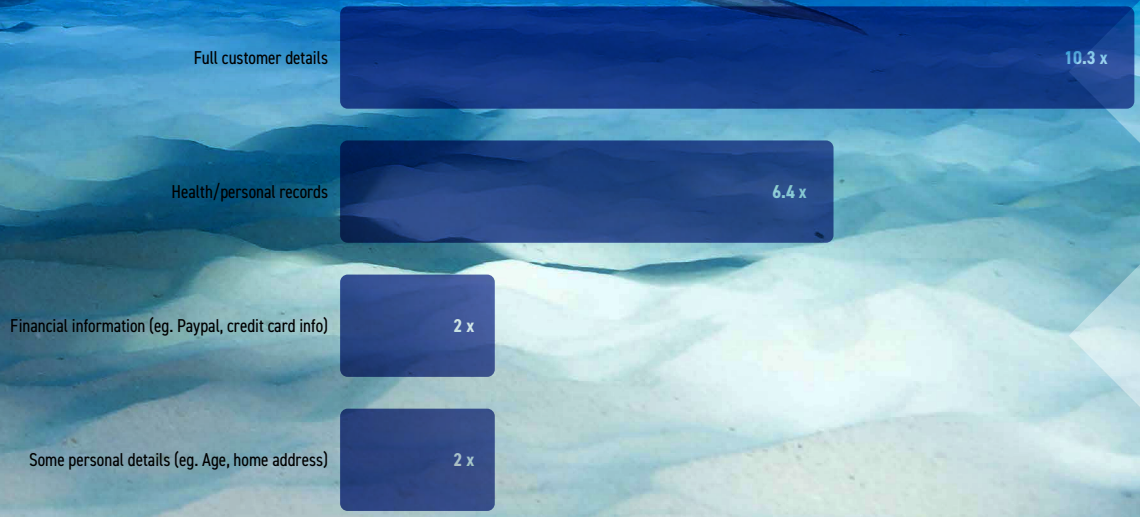
Share price impact by data sensitivity



Media volume:

Does a cyber breach have a pronounced impact on media interest in a company? As you would expect, the answer is yes. On average, a company receives five times more media coverage, and eight times more social media coverage in the month after a cyber breach than in normal conditions. We also see that the bigger the breach and the more sensitive the data, the bigger the media interest.

The size and sensitivity of the data has a bearing on how much interest the media shows



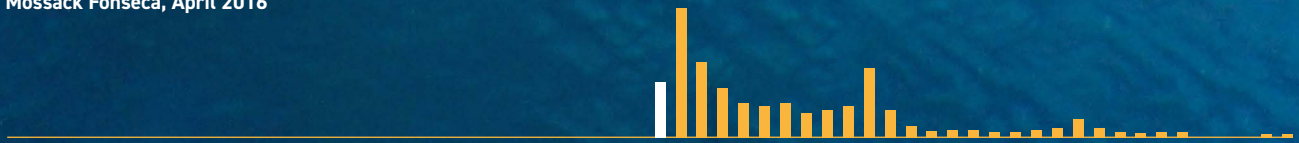
The impact

There are a few interesting outliers here. The largest breaches tend to happen to massive companies who are constantly in the media. As a result, the XXL (100m+) breaches do not show the same increase in interest as those in the XL (10m-100m) category.

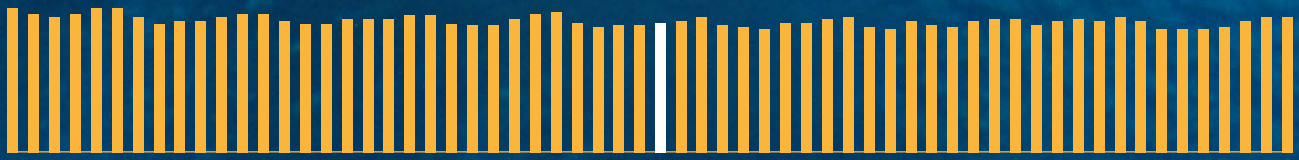
The comparison below between Instagram and Mossack Fonseca represents this idiosyncrasy well. The white line in this chart shows the day of breach announcement. Prior to the news, Mossack Fonseca had no media interest and there was suddenly huge interest after the event. For Instagram, the attack barely registered in terms of volume, even though sentiment would have been impacted.

Previously unknown businesses can see a huge rise in media interest at the point of a breach

Mossack Fonseca, April 2016

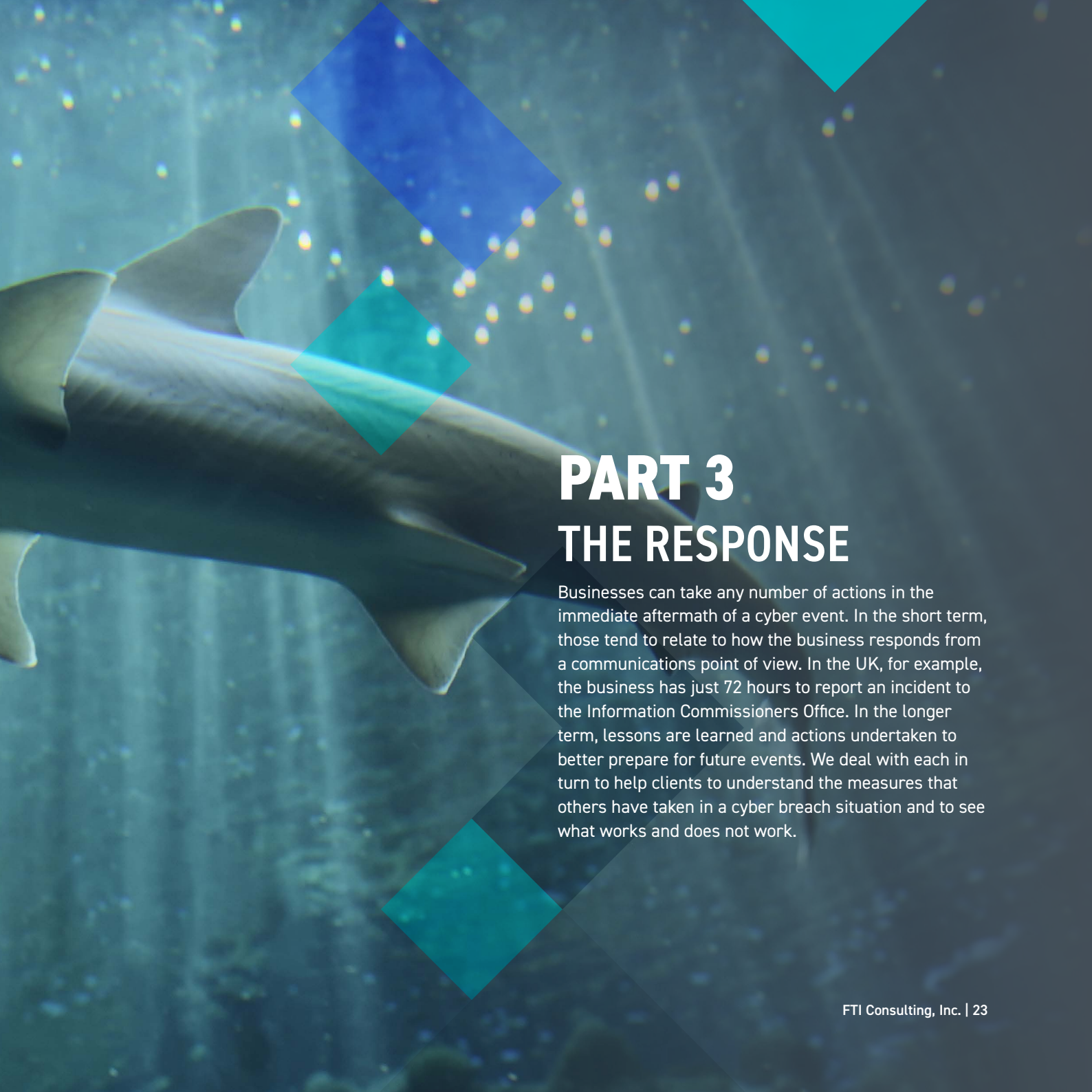


Instagram, September 2017



The lesson for low-profile companies is that a breach can have a disproportionately dramatic effect on the volume of media interest that businesses receive, and it is important to factor surge support into communications planning.

Finally, we wanted to challenge the data to see whether the question of culpability enters the debate. Are companies likely to receive more interest from the media when the incident arises from an internal error versus an external hack? The answer is yes, but only marginally – internal errors receive 10% more attention than external ones.



PART 3
THE RESPONSE

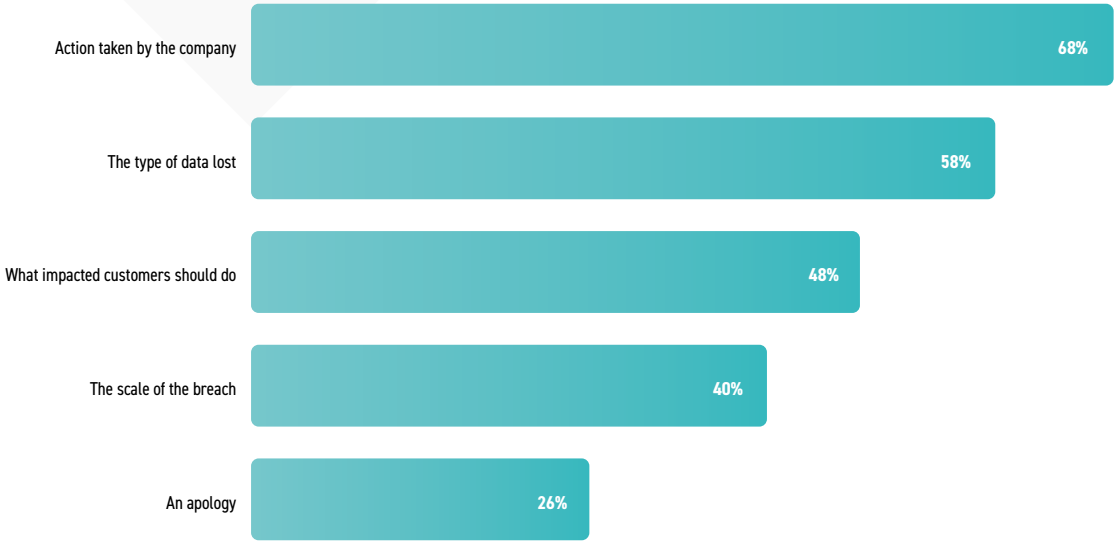
Businesses can take any number of actions in the immediate aftermath of a cyber event. In the short term, those tend to relate to how the business responds from a communications point of view. In the UK, for example, the business has just 72 hours to report an incident to the Information Commissioners Office. In the longer term, lessons are learned and actions undertaken to better prepare for future events. We deal with each in turn to help clients to understand the measures that others have taken in a cyber breach situation and to see what works and does not work.

The response

Short-term response – crisis communications

In 93% of the cases we researched, organisations issued a public statement after an incident. Typically, these statements have five key components, as indicated in the chart below.

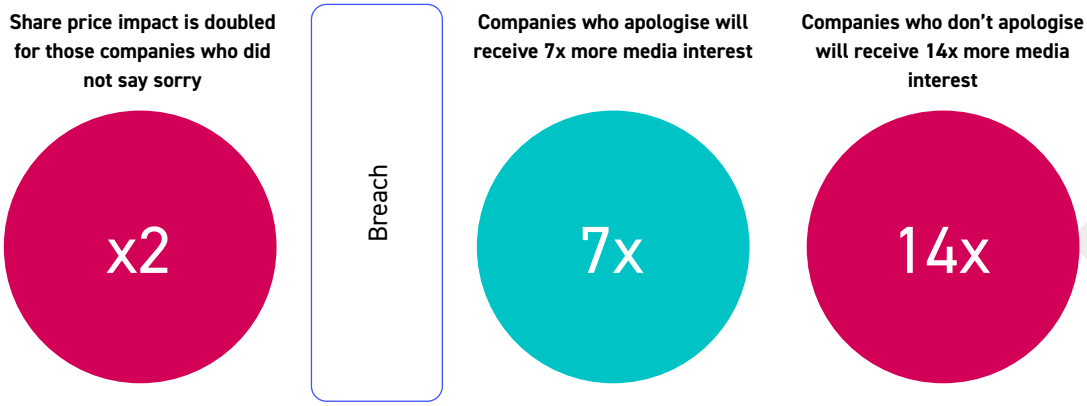
Typical contents of announcements following a breach and how frequently they occur



An apology in the statement and any mention of the scale of the breach seem to be relatively uncommon, compared to other data points. This may be because in the immediate aftermath of a breach, the scale of the breach is unknown, and companies prefer not to guess. As for the apology, companies are clearly wary of saying sorry in the moment, worried about the potential liability that this approach exposes.

However, the research shows that an apology will likely have a calming effect on how the news of the breach is received. The share price decrease on the day of the announcement doubled for those companies who decided not to apologise. Similarly, media interest in companies who do not apologise tends to be double that of those who do say sorry.

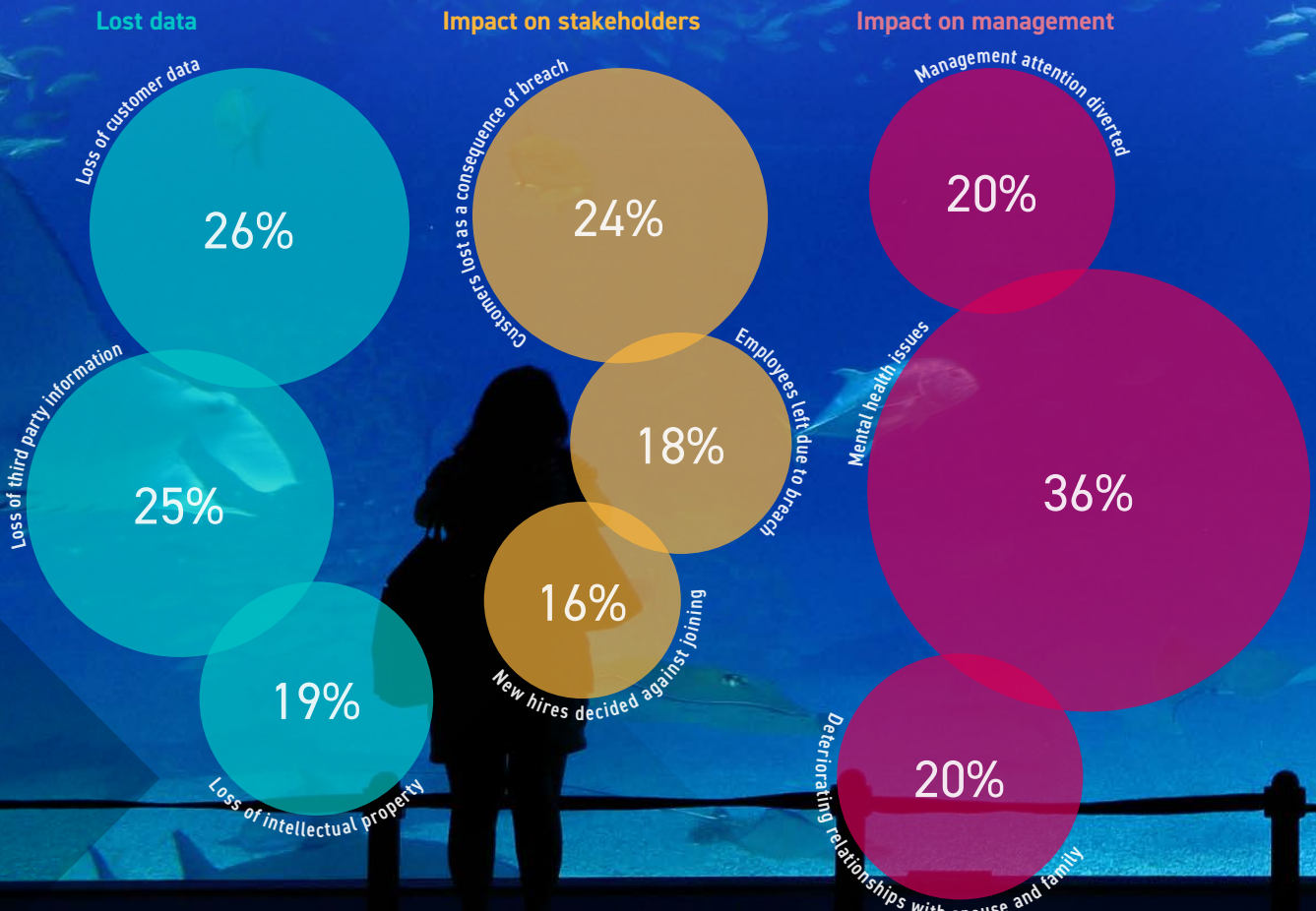
Saying sorry will mean a softer landing



The response

Medium-term response – business preparedness

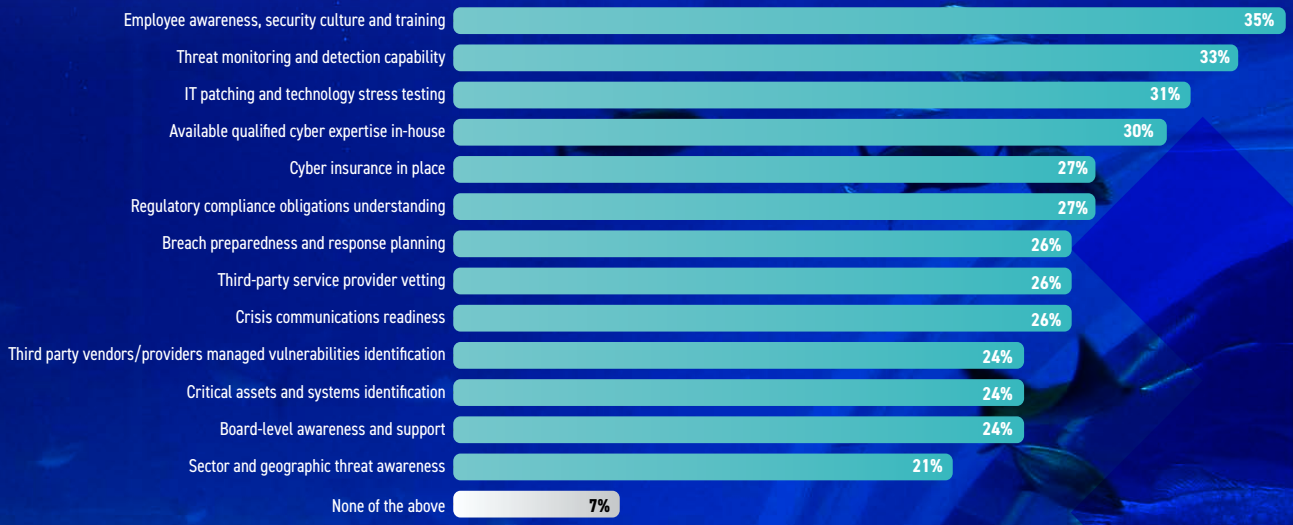
Despite everything that we have learnt previously about the negative impact of a cyber breach and the seriousness that management teams apply to it, it seems that few are preparing to deal with the threat effectively. Only 45% of those we spoke to say that their businesses are preparing proactively to deal with a cyber-attack. And only 39% of business leaders say that their businesses are conducting cyber -attack simulations on a regular basis.



For those businesses which are investing in closing their security gaps, where is the money being spent?

The top investment is in training. 35% of business leaders say that they have invested in employee awareness, security culture and training in the past twelve months – more than any other category. Given the prevalence of internal security breaches that we have seen in Part 1, this focus is understandable. That said, we also noted that lost devices and human error are declining, so these efforts appear to be having a positive effect. Companies clearly understand that training is a responsibility that sits entirely within their control, which is not always the case with certain external elements of cybersecurity.

Which of the following have you invested in over the past 12 months?



When it comes to external threats, the biggest investments are in technology – specifically threat monitoring and detection and IT patching and stress testing. Also high on the list of priorities are activities related to proper governance, namely in-house cyber expertise, cyber insurance and a thorough understanding of regulatory obligations.

Conclusion and recommendations

In today's increasingly connected world, all organisations are at risk from cyber-related threats. A cyber-attack can both cripple operations and damage the reputation of your business.

Our report serves to underline the reality that cyber breaches are an increasingly frequent occurrence in today's world and that the impacts they have are far reaching. It also shows that companies can ameliorate these impacts by preparing and responding appropriately. How companies prepare for a cyber-attack, how they respond to a breach and the lessons they learn in the aftermath are critical factors in ensuring a soft landing.

Before – proactive preparation

Organisations must proactively assess their digital ecosystem to determine additional vulnerabilities. Malicious actors often look for weak spots as access points, and they can leverage connected third-parties to gain entry to their primary target. Cyber resilience involves the protection of internal assets, in addition to identifying and closing any gaps that connected external parties present.

Building a resilient organisation also requires proactive coordination from multiple departments, including senior leadership, instead of leaving cybersecurity to the IT department to handle independently. This holistic approach allows for cybersecurity to be considered as part of strategic decisions, instilling it from the onset versus attempting to address it later.

Given the frequency of breaches which originate from inside the business, culture is also an important element of preparation. Shifting to a proactive mindset when attempting to mitigate cyber risk and become resilient can begin with an organisation's first line of defence – its people. An open and transparent culture will allow issues to be surfaced internally, allowing management teams to respond to cyber risks in their own time and in a more controlled manner. Employee training and awareness form a critical part of any response plan.

Companies should also carefully consider how they plan to respond in the moment of a cyber breach. They must react with speed, proportionality and accuracy to inspire confidence in their customers, employees, investors and regulators that the situation is under control. Social media is increasing the velocity and complexity of every crisis episode and if companies are not well prepared to respond speedily, the situation can quickly get away from them.

This means having a proper communications response plan in place and having well-understood channels of communication within the business, so that the scale and severity of the hack can be quickly understood. This is essential if the company is going to respond properly and accurately - too often we see companies get the facts wrong under pressure to respond promptly.

During – incident response

As we have seen in this report, the reputational impact of a cyber breach can be far reaching, and these days, as much public attention is given to the way a company responds as is to the incident itself. During the pressurised moment of response, in addition to accuracy and speed, the response must also be proportionate. The data in this report provides a guide for management teams to understand how serious their breach is – in terms of size and type – allowing them to see how much attention and concern their breach will attract.

Companies should also consider how well their management teams will respond in these high-pressure moments. Critical business decisions are made at speed, and companies should ask themselves whether they have the right team to respond calmly and accurately to the unfolding drama. Some breach news cycles are over as quickly as they start, but others last for weeks, requiring resilience and stamina from management and communications teams.

A quick and effective response, which satisfies regulatory obligations is critical when it comes to limiting long-term damage. Detection and analysis are also essential to developing an accurate response to the breach. Work will also need to be undertaken to quickly contain and eradicate the threat and then to begin the recovery process.

After – recovery and investigations

Too often companies move quickly back to business as usual in the aftermath of a crisis and do not take time to consider what lessons can be learnt from the incident. It is important that businesses pause for breath and apply their new experience to possible future incidents. What did and did not work and what would the company do differently next time? These are important questions to ask while the experience is still fresh.

With the immediate impact of the breach now behind them, management teams must also turn to the financial, operational and reputational fallout from the crisis. Litigation may be a factor, and preparation will need to begin for that process – again, the accuracy of the data about the breach will be essential. Reputationally, there will be some healing to do. Consideration should therefore be given to the concerns of customers, employees, investors and regulators to reassure, and work will need to begin to regain their trust.

About FTI Consulting's cybersecurity capabilities

Our cybersecurity team consists of over 300 dedicated cybersecurity and communications consultants, led by those with decades of experience at the highest levels of law enforcement, intelligence and global private sector institutions.

We have an integrated team of cybersecurity experts, developers and data analysts with extensive investigative experience. Drawing from both government and the private sector, our experts routinely tackle large-scale analytic challenges requiring complex, custom technical solutions. We regularly contract and leverage technical platforms to collect, analyse and correlate data in demanding environments that require precision and speed. This technical expertise is supported by an international team of communications experts who are well versed in supporting companies as they prepare for and manage the reputational fallout from cyber breaches.

We help clients of any size address their most critical needs and integrate new solutions atop or alongside pre-existing policies and programs to address cyber threats. We build a safer future by helping organisations:

- **Understand their own environments**
- **Harden their defences**
- **Rapidly and precisely hunt threats**
- **Holistically respond to crises**
- **Recover operations and reputation after an event**

Contact details:

UK Crisis Team
+44 (0) 7929 181 850
crisis@fticonsulting.com

Thanks

The completion of this report involved inputs from a wide range of people within the firm. Thanks to Jan Meinicke, Lucy Highland, Greg Hynes, Jack Melling and Jack Hickman for their significant work with the data discovery and analysis. Thanks also to our colleagues in Research – Dan Healy, James Condon and Carole Moyne – for their efforts in pulling together the Resilience Barometer research of business leaders, which formed such a critical part of this study.

About FTI Consulting

FTI Consulting is an independent global business advisory firm dedicated to helping organisations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. Connect with us at www.fticonsulting.com or on Twitter (@FTIConsulting), Facebook and LinkedIn. The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting, Inc. its management, its subsidiaries, its affiliates, or its other professionals, members of employees.

FTI CONSULTING