

# THE IMPACT OF **DATA BREACHES** ON REPUTATION & SHARE VALUE

---

A Study of Marketers, IT Practitioners and Consumers  
in the United Kingdom

---

**Sponsored by Centrify**

Independently conducted by Ponemon Institute LLC

Publication Date: May 2017

# TABLE OF CONTENTS

<b>Introduction .....</b>	<b>01</b>
<b>Executive Summary.....</b>	<b>02</b>
Financial Impact .....	02
Brand Reputation Impact .....	03
Customer Trust Impact.....	04
Additional Business Impact .....	04
<b>Key Findings .....</b>	<b>07</b>
Financial Impact.....	07
Brand Reputation Impact .....	14
Customer Trust Impact.....	17
Additional Business Impact .....	20
<b>Survey Methods and Caveats to this Study .....</b>	<b>23</b>



# INTRODUCTION

*The Impact of Data Breaches on Reputation & Share Value: A Study of Marketers, IT Practitioners and Consumers in the United Kingdom*, conducted by Ponemon Institute and sponsored by Centrifly, examines from the perspective of IT practitioners and marketers how a company's reputation and share value can be affected by a data breach. As part of this research, we surveyed consumers to learn their expectations about steps companies should take to safeguard their personal information and prevent data loss. **This study is unique because it presents the views of three diverse groups who have in common the ability to influence share value and reputation.**

Ponemon Institute surveyed:

# 313

individuals in IT operations and information security (hereafter referred to as IT practitioners)

# 292

senior-level marketers and corporate communication professionals (hereafter referred to as CMOs)

# 405

Consumers

**Forty percent** of IT practitioner respondents and **23 percent** of CMOs in this study say their organisation had a data breach involving the loss or theft of more than 1,000 records containing sensitive or confidential customer or business information in the past two years.



**Fifty-one percent** of consumers say in the past two years they have been notified by a company or government agency that their personal information was lost or stolen as a result of one or more data breaches.

The results of this study show how data loss affects shareholder value and customer loyalty. To protect brand and reputation, it is critical the C-Suite and boards of directors address consumers' expectations about how their personal information is used and secured. Additionally, the study reveals that 39 percent of IT practitioners and 36 percent of CMOs don't believe their senior management understands the importance of preserving the companies' reputation.

# EXECUTIVE SUMMARY

## Financial Impact

### Stock Prices Drop an Average of 5 Percent when the Data Breach is Disclosed

#### The Impact of Data Breaches on Stock Price and Customer Losses

For the economic analysis of the stock price, we selected 113 publicly traded benchmarked companies that experienced a data breach involving the loss of customer or consumer data. We created a portfolio composed of the stock prices of these companies. We tracked the index value for 30 days prior to the announcement of the data breach and 90 days following the data breach.

**The key takeaway from this analysis is that these 113 companies experienced an average stock price decline of 5 percent immediately following the disclosure of their breach.** An additional takeaway is that companies are less likely to see a decline in stock prices if they have a strong security posture through investments in people, process and technologies. Because of their strong security posture, these companies are better able to quickly respond to the data breach. Following are conclusions from this analysis.

- Companies that self-reported their security posture as superior and quickly responded to the breach event recovered their stock value after an average of 7 days.
- In contrast, companies that had a poor security posture at the time of the data breach and did not respond quickly to the incident experienced a stock price decline that on average lasted more than 90 days.
- The difference in the loss of share price between companies with a low security posture and a high security posture averaged 4 percent.
- Organisations with a poor security posture were more likely to lose customers. In contrast, a strong security posture supports customer loyalty and trust.
  - Twenty-seven percent of consumers surveyed say they discontinued their relationship with the company that had a data breach. Of those consumers affected by one or more breaches, 65 percent say they lost trust in the breached organisation.
  - The 113 companies in our sample that experienced a low customer loss rate (less than 2 percent) had an **average revenue loss of £2.08 million**. Organisations that lost more than 5 percent of their customers experienced an average revenue loss of **£3.07 million**.



Companies experienced an average stock price decline of **5%** immediately following the disclosure of their breach



# Both CMOs and IT Agree Top Impact of Breach is Loss of Brand Value and Reputation — Disagree on Brand Responsibility

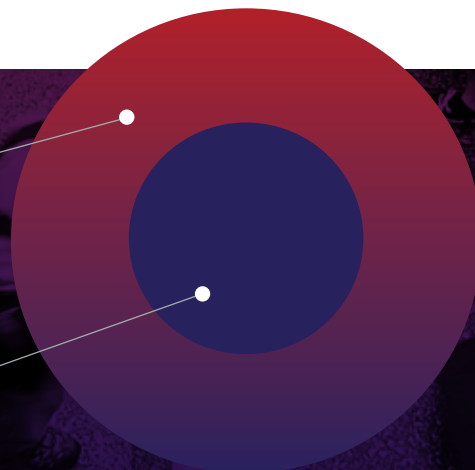
- **Sixty-one percent of CMOs believe the biggest cost of a security incident is the loss of brand value.** In contrast, less than half of IT practitioners (45 percent) see brand diminishment as the biggest cost of a security incident.
- **IT practitioners and CMOs both believe a data breach is a top threat to their companies' reputation and brand value.** A data breach is considered by participants in this research to be a top threat to their companies' reputation and brand value. Unfortunately, 39 percent of IT practitioners and 36 percent of CMOs don't believe that brand protection is taken seriously in the C-Suite.
- **IT practitioners do not believe that brand protection is their responsibility.** Seventy-one percent of IT respondents do not believe protecting their company's brand is their responsibility. However, 43 percent of these respondents do believe a material cyber security incident or data breach would diminish the brand value of their company.
- **CMOs allocate more money in their budgets to brand protection than IT does.** Forty-two percent of CMOs surveyed say a portion of their marketing and communications budget is allocated to brand preservation and 60 percent of these respondents say their department collaborates with other functions in maintaining its brand. Whereas, only 18 percent of IT practitioners say they allocate a portion of the IT security budget to brand preservation and only 18 percent collaborate with other functions on brand protection. This response is understandable because so many IT practitioners do not believe brand protection is the IT function's responsibility.

**61% of CMOs**

believe the biggest cost of a security incident is the loss of brand value

**45% of IT**

practitioners see brand diminishment as the biggest cost of a security incident



# Consumers Expect More Responsibility for Safeguarding Personal Information than Companies are Willing to Assume

- **Consumers' expectation for the security of personal information they share with companies is higher than CMOs and IT practitioners' sense of responsibility.** Seventy-nine percent of consumers believe organisations have an obligation to take reasonable steps to secure their personal information. Sixty-four percent of CMOs and 66 percent IT practitioners agree. The research reveals differences in perceptions between IT practitioners and CMOs on issues regarding reputation and brand management practices. However, more serious differences are the gaps between consumers' expectations and the perceptions of IT practitioners and CMOs about how their personal information should be safeguarded.
- **Less than half of CMOs and IT practitioners believe their organisations have a responsibility to control access to consumers' information.** While 73 percent of consumers surveyed believe organisations have an obligation to control access to their information, 46 percent of CMOs and 44 percent of IT security practitioners believe this is an obligation.
- **Consumer trust in certain industries may be misplaced.** Sixty-eight percent of consumers say they trust healthcare providers to preserve their privacy and to protect personal information. In contrast, only 26 percent of consumers trust credit card companies. Yet, healthcare organisations account for 34 percent of all data breaches while banking, credit and financial organisations account for only 4.8 percent. Banking, credit and financial industries also spend two-to-three times more on cyber security than healthcare organisations.

# 73%

of Consumers

surveyed believe organisations have an obligation to control access to their information

# 46% 44%

of CMOs

of IT practitioners

believe this is an obligation



## Additional Business Impact

# Potential Blindspots and Alignment Costs

- **Seventy percent of IT practitioners do not believe their companies have a high level of ability to prevent breaches.** However, 58 percent of CMOs are confident their company would be resilient to a data breach that results in the loss or theft of high value assets.
- **The loss of stock price is perhaps a blind spot of CMOs and IT practitioners.** Reputation loss due to a data breach is the biggest concern to both IT practitioners and CMOs. However, only 23 percent of CMOs and 3 percent of IT practitioners say they would be concerned about a decline in their companies' stock price. In fact, in organisations that had a data breach, only 5 percent of CMOs and 6 percent of IT professionals say a negative consequence of the breach was a decline in their companies' stock price.
- **IT practitioners and CMOs share the same concern about the loss of reputation as the biggest impact after a breach, but after that, the concerns are specific to their function.** For CMOs, the top three concerns about a data breach are loss of reputation (67 percent of respondents), decline in revenues (53 percent of respondents) and loss of customers (46 percent of respondents). For IT, the biggest concerns are the loss of their jobs (63 percent of respondents), loss of reputation (43 percent of respondents) and time to recover decreases productivity (41 percent of respondents).
- **Following a data breach there is significant financial harm and the IT function comes under greater scrutiny.** IT practitioners in organisations that had a data breach (40 percent) consider the following the most negative consequences of a breach: significant financial harm (52 percent of respondents), greater scrutiny of the capabilities of the IT function (51 percent of respondents), significant brand and reputation damage (35 percent of respondents), and decreased customer and consumer trust in their organisation (35 percent of respondents). CMOs believe that two big problems following a data breach are the decrease in customer and consumer trust in their organisation (56 percent of respondents) and negative media coverage (47 percent of respondents).



Companies' ability to prevent, detect and resolve the consequences of a data breach



# CONCLUSION

The effects of a data breach can ripple throughout the company and have devastating and long-term financial consequences. These include reputation and customer loss, decline in revenues, loss of competitive advantage and employees' inability to be fully productive.

In Part 2 of this report, we provide more analysis of the findings of this research and how having a strong security posture, as measured by Ponemon Institute's Security Effectiveness Score (SES), will reduce the negative consequences of the breach. A company's SES can be improved by having a fully dedicated chief information security officer (CISO), adequate resources, participation in threat sharing programs and strategic investment in appropriate security enabling technologies.

As shown in this research, IT practitioners are not as confident as they should be in their ability to prevent a breach. To increase confidence, a strong security posture that includes an effective data breach response plan is critical. However, to be prepared for the eventual data breach, the C-Suite needs to be actively engaged. Unfortunately, in many cases boards of directors, chairmen and CEOs are avoiding responsibility for data breach preparedness despite the potential for damage to reputation and serious declines in stock value. Since the loss of share value is a very real threat for companies in the aftermath of a data breach, data breach preparedness plans should include procedures for communicating with investors, state attorneys general and regulators.

In addition to making companies more resilient to a data breach with security enabling technologies, consumers' concerns about their personal information should be addressed. As part of data breach preparedness, senior management, especially the chief privacy officer, should be involved in ensuring their company's privacy and data handling practices respect their customers' expectations. Such efforts will help mitigate customer turnover.



## PART 2. KEY FINDINGS

**In this section, we provide an analysis of the key findings.**

We have organised the report according to the following topics:

- Financial Impact
- Brand Reputation Impact
- Consumer Trust Impact
- Additional Business Impact

# FINANCIAL IMPACT

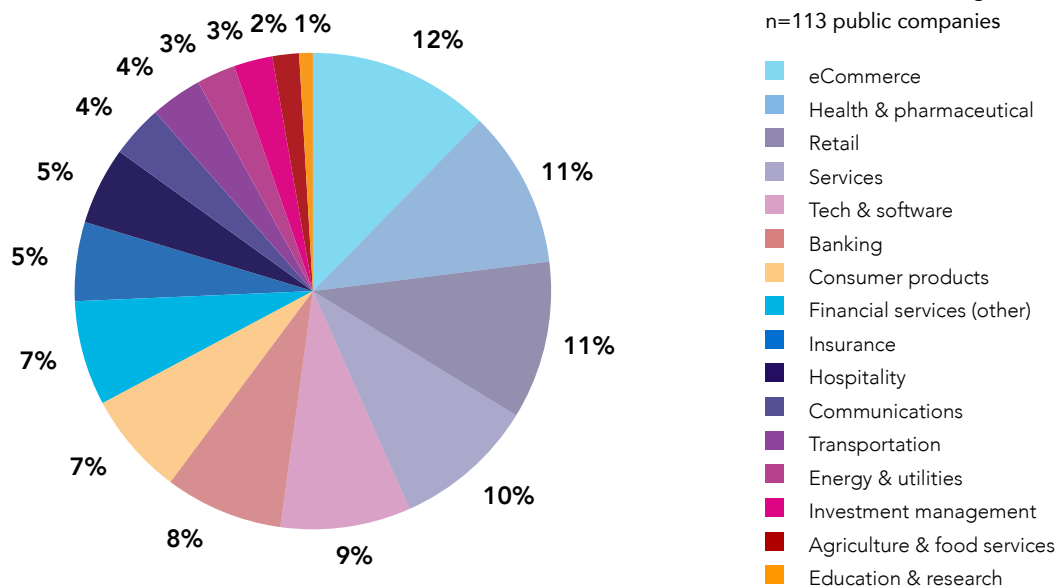
## The Impact of a Data Breach on Share Value

We selected a sample of global data breach cases that were analysed by Ponemon Institute as part of an earlier research project.<sup>1</sup> We selected 113 benchmarked companies that experienced a material data breach. As shown in Pie Chart 1, our final sample contained public companies in 16 industry sectors.

To calculate the impact of a data breach incident on stock price, we first normalised our database of companies.

The 113 companies selected for analysis had data breaches at different points in time. To normalise stock price changes, we looked at the company's stock price 30 days prior to the data breach event and 90 days following the incident. We also normalised stock prices by creating a stock portfolio index (SPI), where \$100 (US Dollar) is the baseline index value set 30 days prior to the event. Thus, UK stock values were converted from British Pounds to US Dollars prior to creation of the SPI.

**Pie Chart 1.** Percentage distribution of the benchmark sample n=113 public companies



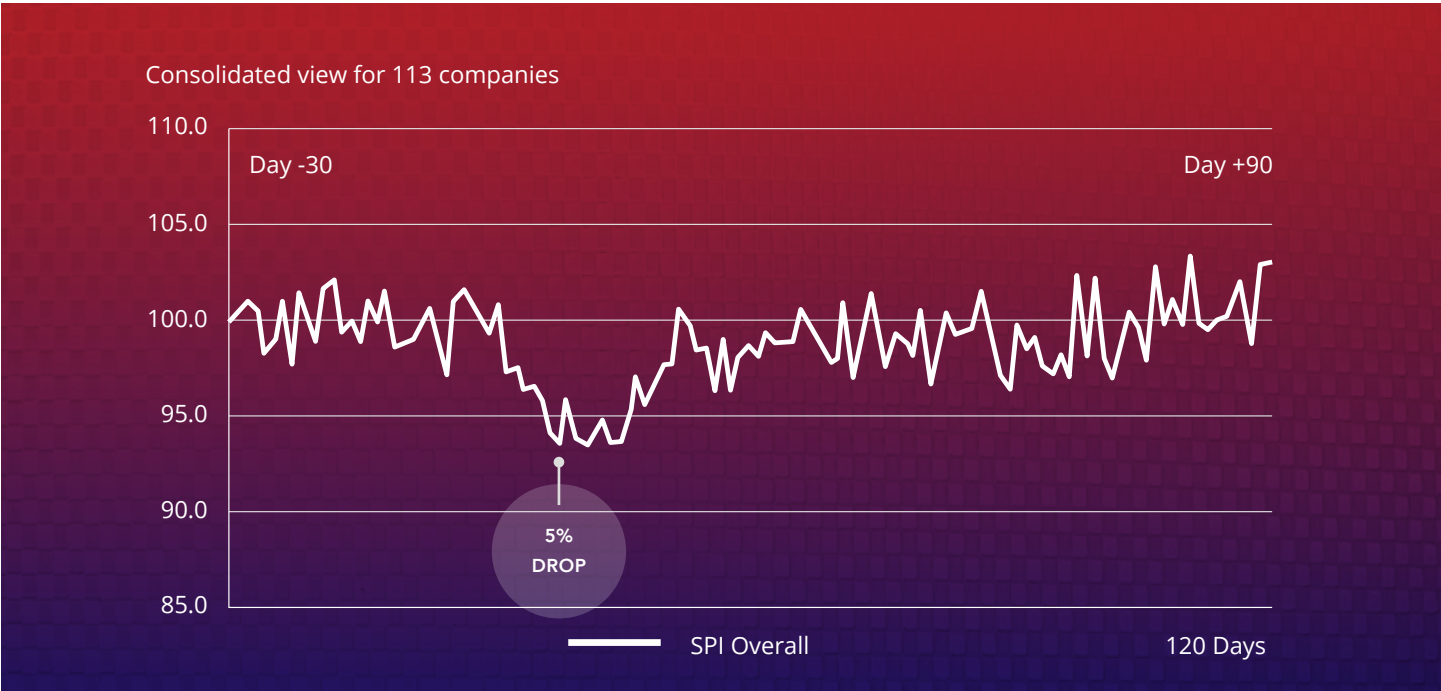
### The criteria for selection of our test sample are as follows:

- The data breach incident involved more than 50,000 records containing sensitive or confidential personal information such as PII, login credentials and payment information.
- The company notified data breach victims and regulators about the incident.
- The company was publicly traded on a major exchange at the time of the breach.
- The company completed the Security Effectiveness Scoring (SES) method soon after containing the incident.



There is a clear and direct correlation between a data breach and stock decline. Figure 1 shows that the share price index declines soon after a material data breach event is publicly disclosed (day 0). The figure suggests a full recovery in index value about 45 days following the event.

Figure 1. Share portfolio index over 120 days



For illustration purposes, Table 1 presents two data breach cases in the UK from our 113 companies in two different industries. These companies are all publicly traded. For purposes of confidentiality, we do not disclose company-identifiable information.

Table 1. Two cases

INDUSTRY	FINANCIAL SERVICES	RETAIL
LOCATION	U.K.	U.K.
TURNOVER RATE	2.11%	2.54%
STOCK PRICE DECLINE	5.6%	0.88%
DAYS TO RECOVER	85	116

# Measuring Security Posture

---

To understand how stock price can be affected following a data breach, we bifurcated the companies according to their security posture, which is measured by the Security Effectiveness Score (SES). This proprietary methodology was developed by Ponemon Institute for its annual encryption trends survey to define the security posture of responding organisations. The SES is derived from the rating of numerous security features or practices.

This method has been validated from more than 50 independent studies conducted for more than a decade. The SES provides a range of +2 (most favorable) to -2 (least favorable) with a theoretical mean of zero. Hence, a score greater than zero is viewed as net favorable and a score less than zero is net unfavorable.

A high favorable score (such as +1 or above) indicates that the organisation's investment in people and technologies is both effective in achieving its security mission and is efficient.

Data breaches are pervasive and companies with both a positive and negative security posture can experience the loss or theft of sensitive and confidential information. However, it is our belief that companies with a strong security posture are more resilient, and therefore will have a less detrimental impact on stock price than those with a weak security posture. Of the 113 companies, 57 had an average favorable score of +.67 and 56 had an average unfavorable score of -.71. Following are attributes of both a high and low SES.

## Security Effectiveness Score Attributes

### High SES

- Fully dedicated CISO
- Adequate budget for staffing and investment in enabling security technologies
- Strategic investment in appropriate security enabling technologies, especially enterprise-wide encryption
- Training and awareness programs designed to reduce employee negligence
- Regular audits and assessments of security vulnerabilities
- A comprehensive program with policies and assessment to manage third-party risk
- Participation in threat sharing programs

### Low SES

- Lack of incident response plans
- Inadequate funding for staffing and investment in enabling security technologies
- Frequent turnover of IT security personnel
- Poor data retention practices
- The C-Suite values productivity of workforce over security
- Lack of collaboration between lines of business and IT security in determining IT security priorities



# The Relationship Between Share Value and a Strong Security Posture

**Stock values in high security posture companies recover faster after a breach.** As shown in Figure 2, companies with a high security posture had a stock value decline of no more than 3 percent following disclosure of the breach (day 0). Ninety days following the breach, the stock index value showed a gain of 3 percent above what the stock price was before the breach.

Companies with a high (superior) security posture show a quick reaction to the data breach event, and stock value recovers after only seven (7) days. In contrast, low security posture companies' stock price does not fully recover after a breach. Companies with a low (poor) security posture experience a stock price decline after the data breach disclosure, and this decline appears to be long lasting (e.g., more than 90 days).

**Figure 2.** Comparison of high vs. low Security Effectiveness Score (SES) subsamples over 120 days

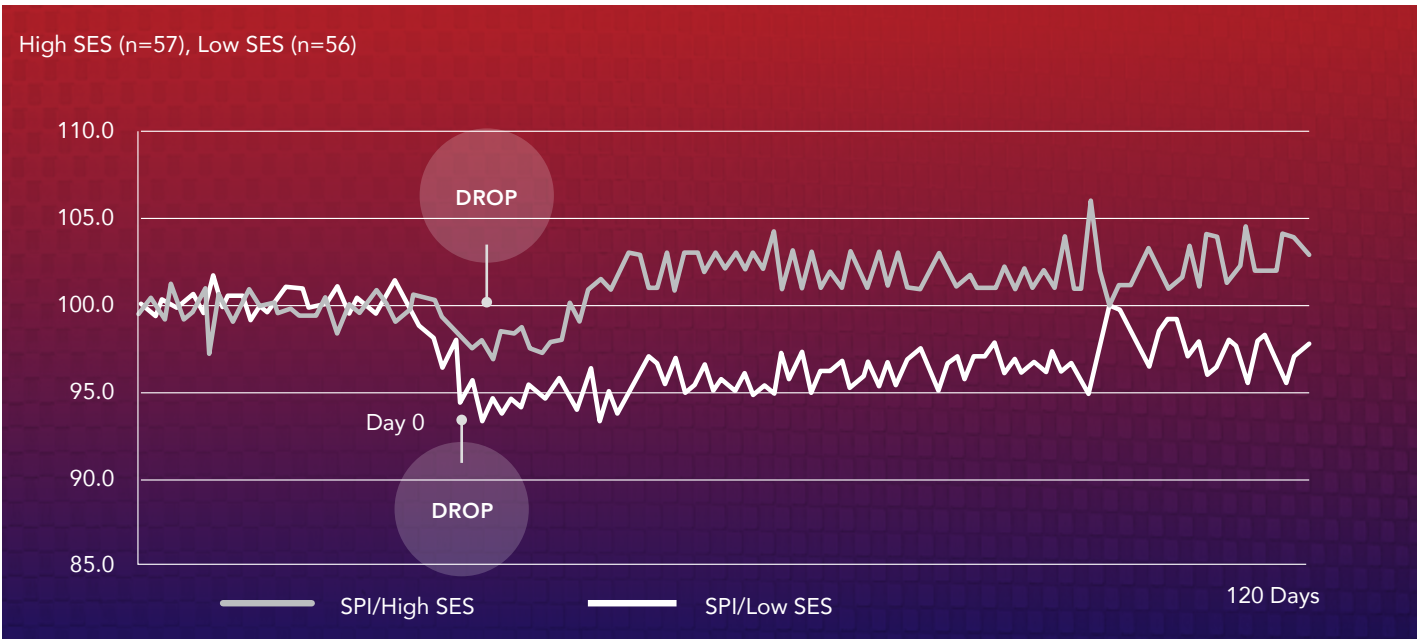


Table 2 shows statistically significant differences between low and high SES groups. In general, the data breach event was more detrimental for companies in the low SES group.

The average difference in index values between low and high SES companies is \$3.9 or (4 percent). Furthermore, low SES companies experience a long-lasting dip in index value following the breach event.

**Table 2.**

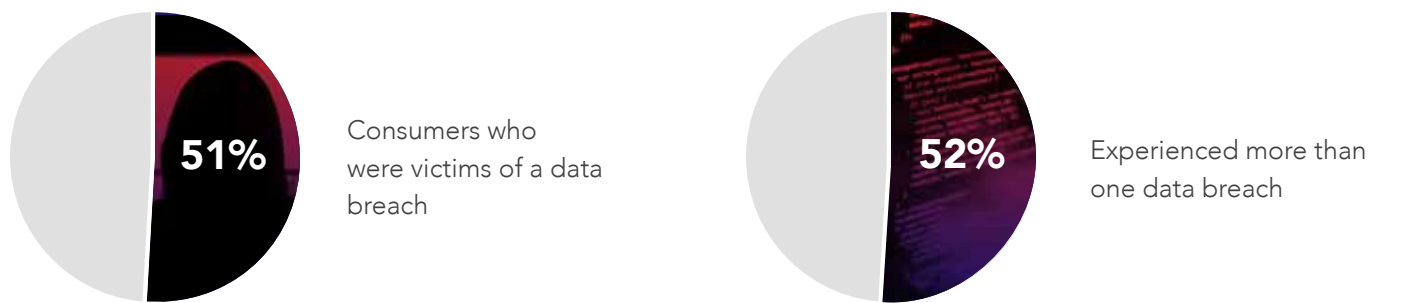
KEY STATISTICS	SPI / HIGH SES	SPI / LOW SES	SPI OVERALL
Average	101.0	97.2	98.9
Median	101.0	96.8	99.1
Maximum	106.0	101.6	103.4
Minimum	97.0	93.1	93.8
Ending index value (day 120)	103.0	97.6	103.0
Difference in average SPI for low and high SES groups			\$3.9
Percentage difference (delta)			4%

# The Relationship Between Customer Turnover and a Strong Security Posture

Consumers have an impact on an organisation’s reputation and brand following a breach. Fifty-one percent of consumers in this study were victims of a data breach and 52 percent of these respondents say they were the victims of more than one. These multiple breaches have had a serious impact on the relationship the consumer has with the organisation. According to

Figure 3, 65 percent of respondents say these incidents did cause them to lose trust in the organisation experiencing the data breach. Twenty-seven percent say they actually took steps to terminate their relationship with the breached organisation. Eleven percent of respondents say the data breach resulted in a criminal act such as credit card fraud or identity theft.

Figure 3.



## How did the data breach affect you?



Figure 4. Churn rate following a breach by Security Posture (SES)

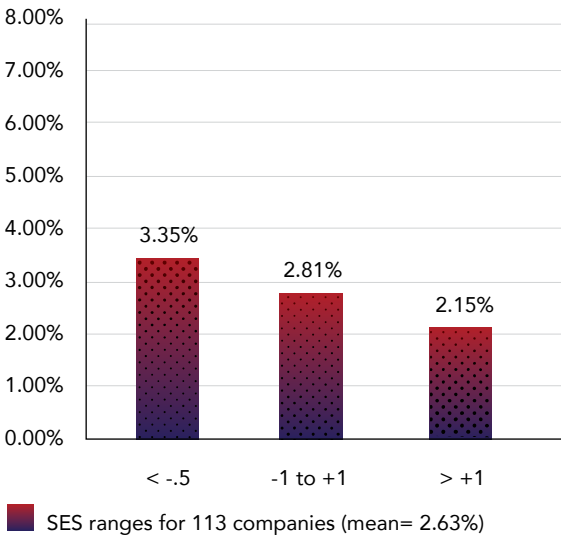


Figure 4 shows an inverse relationship between SES ranges and percentage customer turnover. Specifically, organisations with a negative SES experienced a higher customer loss rate (3.35 percent). Those with a positive SES experienced a lower customer loss rate (2.15). The average customer loss rate for our sample of 113 companies is 2.63 percent. The range is from 0 (no turnover) to 7 percent.

2.15%

Customer loss rate with positive SES

3.35%

Customer loss rate with negative SES

Figure 5. Average revenue loss due to breach by churn rate

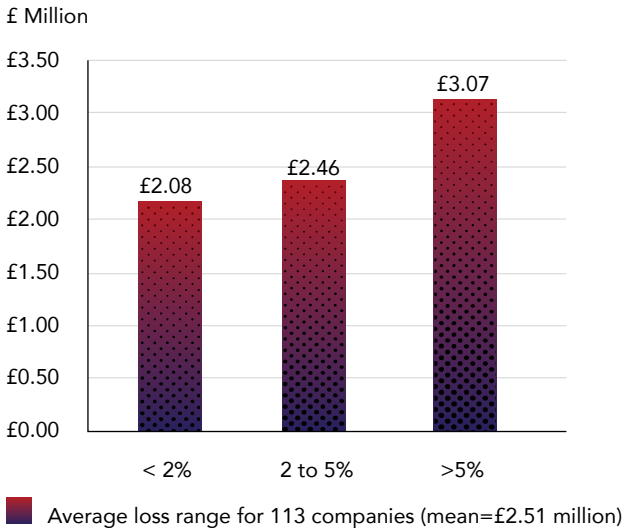


Figure 5 shows the relationship between customer turnover and average business losses. Specifically, organisations with a high turnover rate experienced a much higher business loss (£3.07 million), and those with a low turnover experienced a lower business loss (£2.08 million). The average business loss for our sample of 113 companies is £2.51 million. The range is from £0.4 million to £11 million.

£2.08M

The average revenue loss for low turnover rates

£3.07M

The average revenue loss for high turnover rates

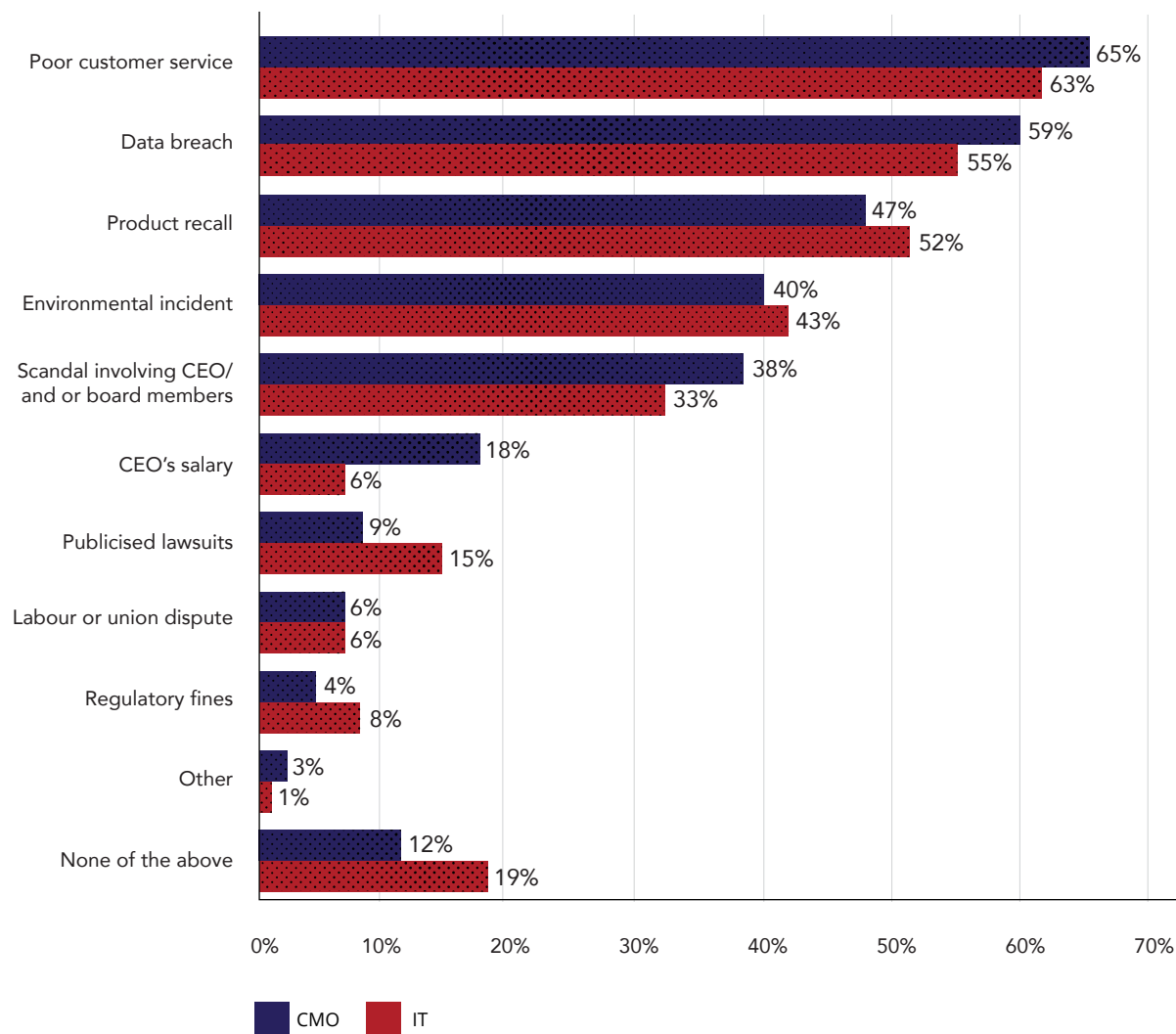


# BRAND REPUTATION IMPACT

## Reputation and Brand Management

**A data breach is one of the top three negative effects on brand reputation.** As shown in Figure 6, both IT security (55 percent of respondents) and CMOs (59 percent of respondents) believe a data breach and product recall would have a negative impact on their brand reputation, a ranking above the potential impact of a scandal involving the CEO. The most serious threat to reputation is poor customer service ( 65 percent of CMOs and 63 percent of IT practitioners).

**Figure 6.** Which of the following issues would most likely have a negative impact on your organisation's reputation?  
Please select the top three choices

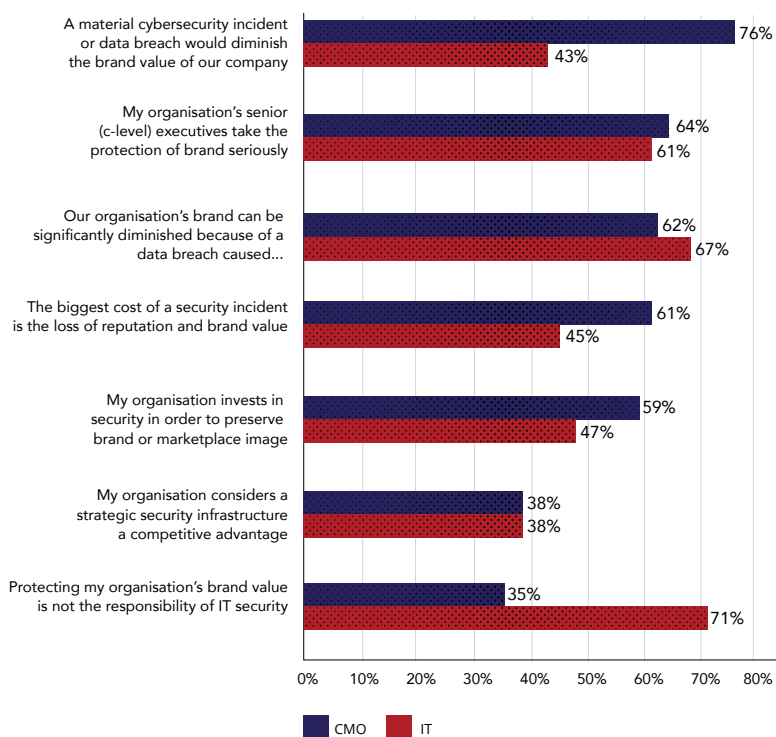


**CMOs are more concerned than IT practitioners about the preservation of their companies' brand and reputation.** CMOs in this research have at least some involvement in programs to support their companies' brand and reputation. Whereas, IT practitioners probably believe their primary role is protecting their organisation's sensitive and confidential information. Consequently, as shown in Figure 7, most IT practitioners (71 percent) **do not** believe that brand protection is their responsibility.

However, CMOs would like IT practitioners to take more responsibility. Only 35 percent of CMOs believe protecting brand reputation **is not** the responsibility of IT security. In other words, 65 percent of CMOs believe they should take responsibility. Thirty-nine percent of IT practitioners and 36 percent of CMOs don't believe that brand protection is taken seriously in the C-Suite. Sixty-one percent of CMOs in this study believe the biggest cost of a security incident is the loss of reputation and brand value. In contrast, less than half of IT practitioners (45 percent) agree with this perception.

There are other interesting differences between CMOs and IT practitioners in perceptions about the relationship between reputation and security. Only 43 percent of IT practitioners do recognise a material cybersecurity incident or data breach would diminish the brand value of their company, but a much higher percentage of CMOs (76 percent) believe a material breach is a threat to brand value. Very few CMOs and IT practitioners are likely to believe a strategic security infrastructure is a competitive advantage (both 38 percent of CMOs and IT practitioners).

**Figure 7. Perceptions about the relationship between reputation and security**



CMOs invest more in the preservation of brand.

According to Figure 8, CMOs are more likely to have budget and collaborate with other functions to preserve their company's brand.

As shown in Figure 8, only 18 percent of IT respondents say a portion of the IT security budget is allocated to brand preservation and only 18 percent say they collaborate with other functions in maintaining the company's brand. This is understandable based on their belief that it is not their responsibility to protect their company's brand.

An average of \$9.7 million is spent on IT security in the companies represented in this study and an average of 16 percent of the IT security budget is allocated to the preservation of their company's brand value. A higher percentage (18 percent) is allocated to identity and access management.

Figure 8. How IT security & marketing supports brand preservation

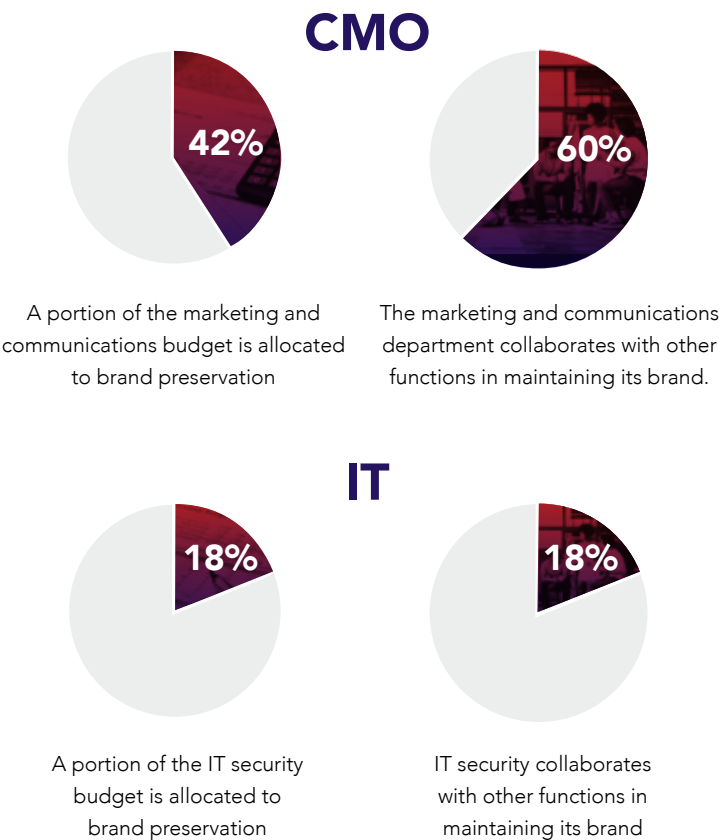


Table 3.

Allocation of Resources to Protect Brand and Invest in IAM	
IT security budget	£9,700,000
Budget allocated to the preservation of brand	£1,520,000
Budget allocated to identity and access management	£1,770,000



## CUSTOMER TRUST IMPACT

# There is a Privacy and Security Expectations Gap Between Consumers and Companies

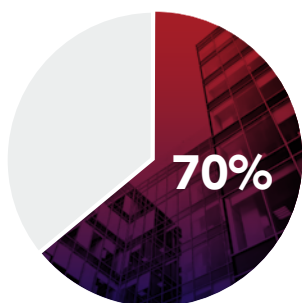
Consumers in this research are aware of the prevalence of data breaches — either from firsthand experience or media reports.

The impact of this awareness is shown in Figure 9. We asked consumers to rate three areas related to the protection and privacy of their personal information on a scale from 1 = low to 10 = very high:

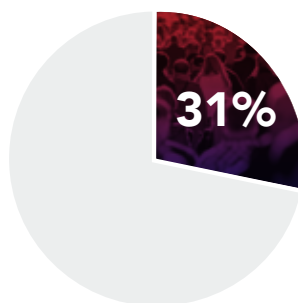
1. The importance of security and privacy practices
2. The ability of companies and government to protect personal information
3. The level of control consumers have over the privacy and security of their personal information

Seventy percent of respondents say a company's privacy and security practices are very important to preserving their trust. However, only 31 percent believe companies and governmental organisations are able at a high level to protect their personal information and only 19 percent of respondents believe they have a high level of control over the privacy and security of their information.

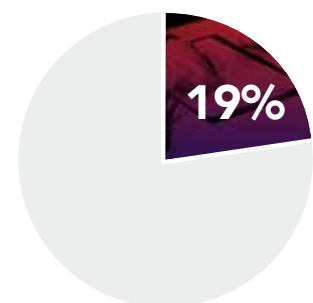
**Figure 9.** What do consumers think about the privacy and protection of their personal information?



The importance of privacy and security practices for preserving trust in the companies and governmental organisations you deal with



The ability of companies and governmental organisations to protect your personal information



The level of control consumers have over the privacy and security of their personal information

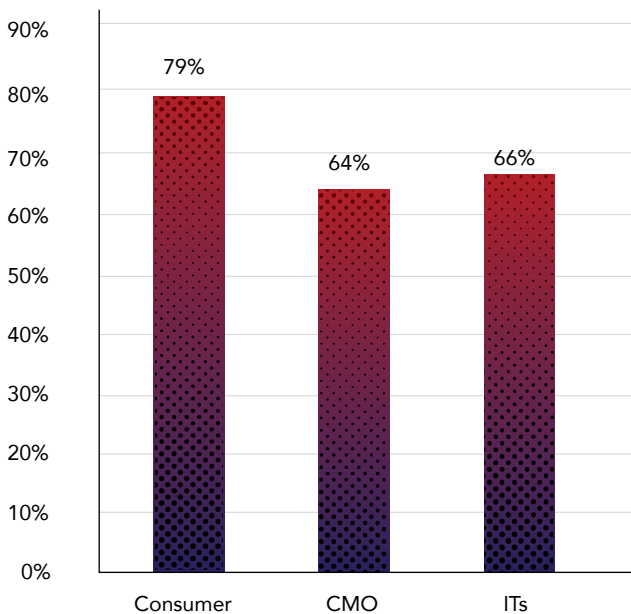
# 79%

of consumers believe organisations have an obligation to take reasonable steps to secure their personal information.

**Consumers' expect control over how companies use their personal information.** They also expect companies to take appropriate steps to protect the privacy and security of their information.

As shown in Figure 10, 79 percent of consumers believe organisations have an obligation to take reasonable steps to secure their personal information. In contrast to other expectations, more CMOs and IT security practitioners agree with consumers (64 percent of respondents and 66 percent of respondents, respectively).

**Figure 10.** Organisations have an obligation to take reasonable steps to secure personal information

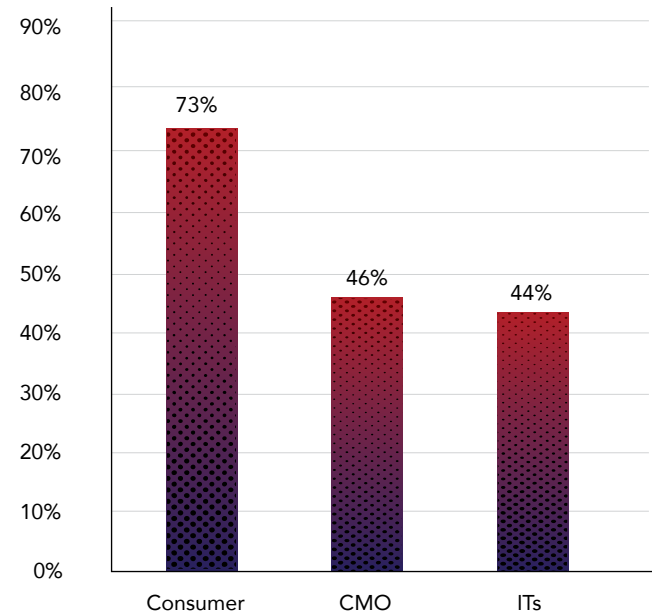


# 73%

of consumers believe organisations have an obligation to control access to their information.

**Organisations feel even less responsibility regarding access to consumer information.** Figure 11 shows 73 percent of consumers believe organisations have an obligation to control access to their information, less than half of CMOs and IT security practitioners believe this is an obligation.

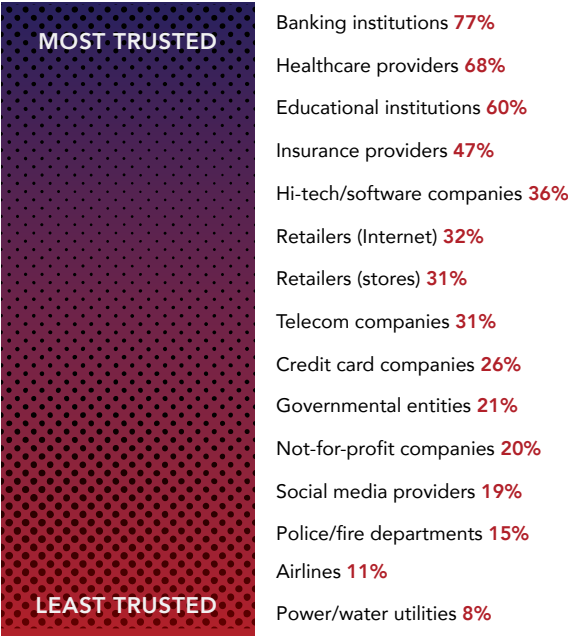
**Figure 11.** Organisations have an obligation to control who has access to personal information



**Few consumers trust social media for privacy and data protection.** As shown in Figure 12, the least trusted organisations are social media providers (19 percent of respondents), police/fire departments (15 percent of respondents), airlines (11 percent of respondents) and power/water utilities (8 percent of respondents).

Healthcare providers and banks are considered most trustworthy for preserving their privacy and protecting their personal information. Seventy-seven percent of respondents say they trust banking institutions the most and 68 percent of respondents say healthcare providers are most trustworthy. Also trusted are educational institutions, according to 60 percent of respondents.

**Figure 12.** Which types of organisations do you trust to preserve privacy and protect personal information? Five choices permitted



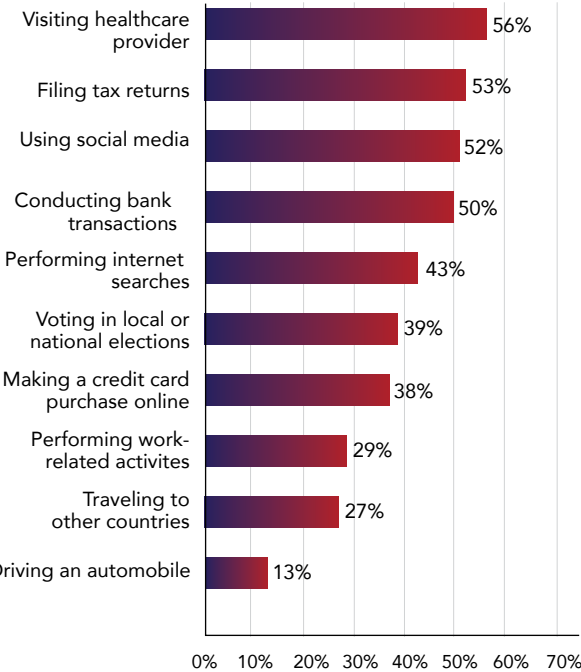
While consumers trust healthcare two times more than credit card companies, healthcare organisations account for 34 percent of all data breaches (and 44 percent of all breached records).<sup>2</sup>

By comparison, banking, credit and financial organisations account for only 4.8 percent (and only 0.2 percent of all records)<sup>3</sup>, but they also spend two-to-three times more on cyber security than healthcare organisations.<sup>4</sup>

Privacy and security is very important when using social media, as shown in Figure 13. Unfortunately, very few respondents trust their social media providers.

Fifty-six percent of respondents believe privacy and security is most important when visiting healthcare providers and filing tax returns.

**Figure 13.** When is your privacy and security most important to you? Four choices permitted



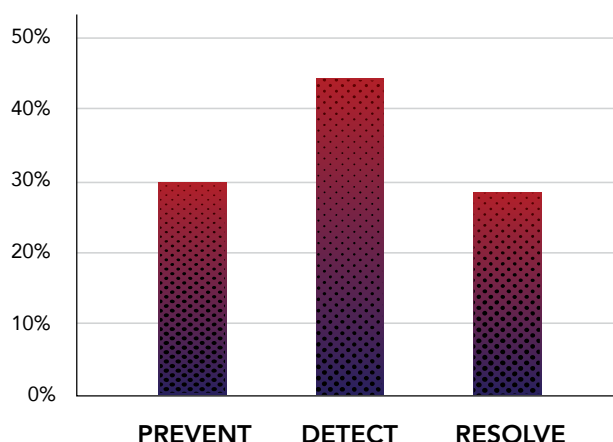


## ADDITIONAL BUSINESS IMPACT

### Potential Blindspots and Alignment Costs

**Those in the IT trenches give their companies low marks in preventing, detecting and managing the consequences of data breaches.** We asked IT practitioners to rate their organisations' ability to prevent, detect and resolve a data breach from a scale of 1 = no ability to 10 = high ability. As shown in Figure 14, only 30 percent rate their companies' ability to prevent a data breach as high (7+ on a scale of 1 = low ability to 10 = high ability) and 44 percent of respondents rate their ability to quickly detect a data breach as high. Only 29 percent of respondents rate their organisations' ability to quickly resolve the consequences of a data breach as high.

**Figure 14.** Companies' ability to prevent, detect and resolve the consequences of a data breach

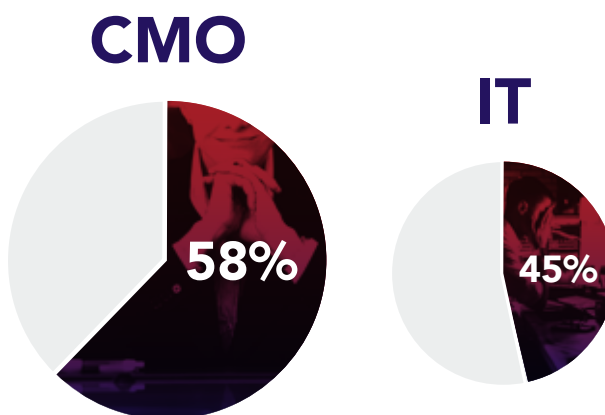


**CMOs are more optimistic about their companies' ability to successfully survive the consequences of a breach of high value assets.** We asked respondents to rate their organisations' resiliency to a data breach involving high value assets on a scale of 1 = low resilience to 10 = high resilience.

Figure 15 presents the 7+ responses, indicating a belief that their organisations are highly resilient. Fifty-eight percent of CMOs say their companies are highly resilient to a data breach involving high value assets. In contrast, only 45 percent of IT respondents are confident in their organisations' resiliency.

In the context of this study, high value assets are defined as the confidential information critical to the development, performance and marketing of a company's core businesses. These assets may include trade secrets, corporate confidential information and personal information about customers, business partners, employees and other key stakeholders.

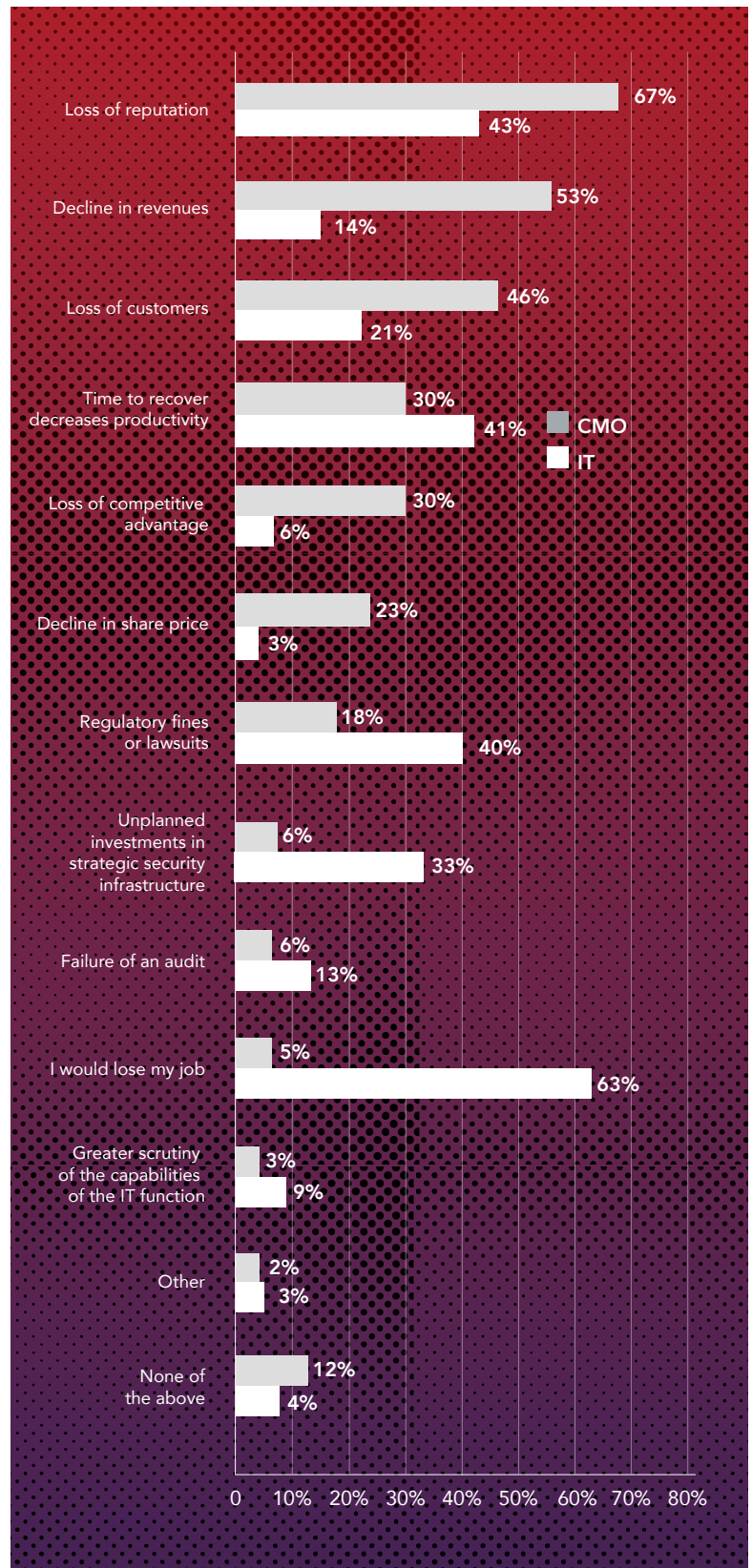
**Figure 15.** How resilient is your organisation to a data breach that causes the loss or theft of high value assets?



## The loss of stock price is possibly a blind spot for CMOs and IT practitioners

As shown in Figure 16, the biggest concern to both IT practitioners and CMOs if their organisation had a data breach is the loss of reputation. Only 23 percent of CMOs and 3 percent of practitioners say it would be a decline in stock price. In fact, in organisations that had a data breach, only 5 percent of CMOs and 6 percent of IT practitioners say a negative consequence of a data breach was a decline in stock price.

**Figure 16.** What are your biggest concerns if your company has a data breach? Three choices permitted

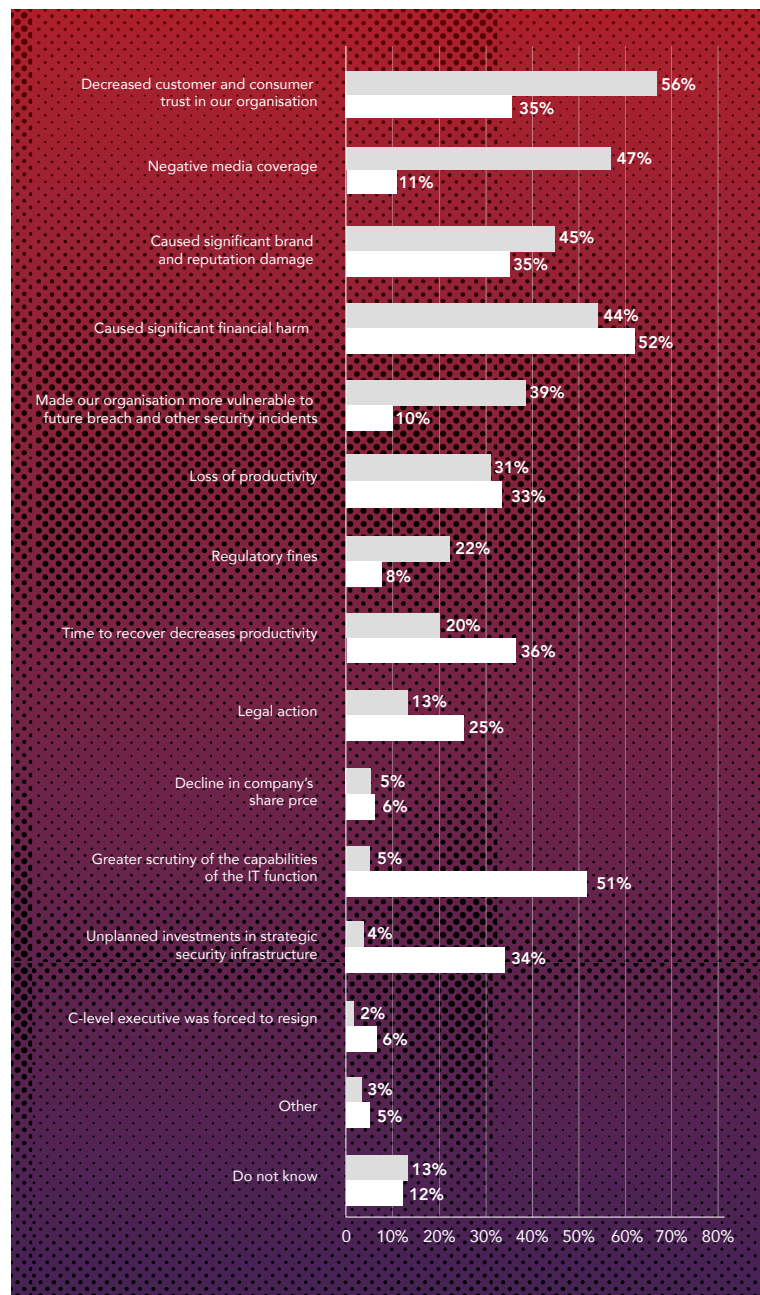


## When a data breach occurs, CMOs and IT practitioners have different perceptions about the most negative consequences

Fifty-six percent of CMOs believe the most serious consequence is decreased customer and consumer trust in their organisations, 47 percent say it is negative media coverage and 45 percent say it caused significant brand and reputation damage, as shown in Figure 17.

However, 52 percent of IT practitioners say the breach caused significant financial harm and 51 percent say it was the pressure of increased scrutiny following the data breach.

**Figure 17.** What were the negative consequences of a data breach?  
More than one choice permitted





# PART 3.

## SURVEY METHODS AND CAVEATS TO THIS STUDY

### Survey Methods

This report consists of three sets of survey responses. The first group of participants is a sampling frame of 9,803 individuals in IT security and IT operations. Table 4 shows 364 total returns. Reliability checks required the removal of 51 surveys. Our final sample consisted of 313 surveys, or a 3.2 percent response rate.

The second group of participants is a sampling frame of 5,883 individuals who are CMOs and corporate communication professionals. Table 4 shows 331 total returns. Reliability checks required the removal of 39 surveys. Our final sample consisted of 292 surveys, or a 5.0 percent response rate. The third group of participants is a sampling frame of 12,982 consumers. Table 4 shows 465 total returns. Reliability checks required the removal of 60 surveys. Our final sample consisted of 405 surveys, or a 3.1 percent response rate.

Table 4.

SAMPLE RESPONSE: U.K.	IT	CMO	CONSUMER
Sampling frame	9,803	5,883	12,982
Total returns	364	331	465
Rejected surveys	51	39	60
Final sample	313	292	405
Response rate	3.2%	5.0%	3.1%

# Caveats to this Study

---

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

- **Non-response bias:** The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.
- **Sampling-frame bias:** The accuracy is based on contact information and the degree to which the list is representative of IT practitioners, CMOs and consumers. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.
- **Self-reported results:** The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate or truthful responses.

For more information about this study, please contact Ponemon Institute by sending an email to **research@ponemon.org** or calling our toll free line at **1.800.887.3118**.



## Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organisations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

<sup>1</sup> The source of these actual data breach cases is Ponemon Institute's global cost of data breach research, sponsored by IBM. See 2016 Cost of Data Breach: Global, published June 2016.

<sup>2</sup> [http://www.idtheftcenter.org/images/breach/2016/DataBreachReport\\_2016.pdf](http://www.idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf)

<sup>3</sup> [http://www.idtheftcenter.org/images/breach/2016/DataBreachReport\\_2016.pdf](http://www.idtheftcenter.org/images/breach/2016/DataBreachReport_2016.pdf)

<sup>4</sup> <https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697>



As the only industry recognised leader in both Privileged Identity Management and Identity-as-a-Service, Centrify provides a single platform to secure every user's access to apps and infrastructure in today's boundaryless hybrid enterprise through the power of identity services. This is the Next Dimension of Security in the Age of Access.

Founded in 2004, Centrify is enabling over 5,000 customers, including over half the Fortune 50, to defend their organisations. Centrify is a privately held company based in Santa Clara, California. To learn more visit [www.centrify.com](http://www.centrify.com).

**The Breach Stops Here.**