Ponemon INSTITUTE

2017 Cost of Data Breach Study

South Africa

Benchmark research sponsored by IBM Security
Independently conducted by Ponemon Institute LLC
June 2017

Ponemon Institute©
Research Report

IBM Security

2017 Cost of Data Breach Study: South Africa

Ponemon Institute, June 2017

Part 1. Introduction

IBM Security and Ponemon Institute are pleased to present the *2017 Cost of Data Breach Study: South Africa*[1] our second benchmark study on the cost of data breach incidents for companies located in South Africa. The average per capita cost of data breach was 1,632 ZAR and the average total organisational cost was 32.36 million ZAR. To date, 40 South African organisations have participated in this research.

Ponemon Institute conducted its first *Cost of Data Breach Study* in the United States 12 years ago. Since then we have expanded the research to the following countries and regions:

- The United Kingdom
- Germany
- Australia
- France
- Brazil
- Japan
- Italy
- India
- Canada
- South Africa
- The Middle East (including the United Arab Emirates and Saudi Arabia)
- ASEAN region (including Singapore, Indonesia, the Philippines and Malaysia)

South Africa at a glance

- 21 South African companies participated
- 32.36 million ZAR is the average total cost of data breach
- 12% increase in the total cost of data breach
- 1,632 ZAR is the average cost per lost or stolen record
- 5% increase in the cost per lost or stolen record

The 2017 study examines the costs incurred by 21 South African organisations from nine different industry sectors following the loss or theft of protected personal data and the notification of breach victims as required by various laws. It is important to note that costs presented in this research are not hypothetical but are from actual data loss incidents. The costs are based on estimates provided by the individuals interviewed over a 10-month period in the companies represented in this research.

The number of breached records per incident this year ranged from 2,400 to 76,900 and the average number of breached records was 19,800. We did not recruit organisations that have data breaches in excess of 100,000 compromised records. These incidents are not indicative of data breaches most organisations incur. Thus, including them in the study would have skewed the results.

Why the cost of data breach fluctuates across countries

What explains the significant increases in the cost of data breach this year for organisations in the Middle East, the United States and Japan? In contrast, how did organisations in Germany, France, Australia, and the United Kingdom succeed in reducing the costs to respond to and remediate the data breach? Understanding how the cost of data breach is calculated will explain the differences among the countries in this research.

For the *2017 Cost of Data Breach Study: Global Overview*, we recruited 419 organisations in 11 countries and two regions to participate in this year's study. More than 1,900 individuals who are

[1] This report is dated in the year of publication rather than the year of fieldwork completion. Please note that the majority of data breach incidents studied in the current report happened in the 2015 calendar year.

knowledgeable about the data breach incident in these 419 organisations were interviewed. The first data points we collected from these organisations were: (1) how many customer records were lost in the breach (i.e. the size of the breach) and (2) what percentage of their customer base did they lose following the data breach (i.e. customer churn). This information explains why the costs increase or decrease from the past year.

In the course of our interviews, we also asked questions to determine what the organisation spent on activities for the discovery of and the immediate response to the data breach, such as forensics and investigations, and those conducted in the aftermath of discovery, such as the notification of victims and legal fees. A list of these activities is shown in Part 3 of this report. Other issues covered that may have an influence on the cost are the root causes of the data breach (i.e. malicious or criminal attack, insider negligence or system glitch) and the time to detect and contain the incident.

It is important to note that only events directly relevant to the data breach experience of the 419 organisations represented in this research and discussed above are used to calculate the cost. For example, new regulations, such as the General Data Protection Regulation (GDPR), ransomware and cyber attacks, such as Shamoon, may encourage organisations to increase investments in their governance practices and security-enabling technologies but do not directly affect the cost of a data breach as presented in this research.

The calculation of the components of the cost of data breach that affect the cost

The following information presents the data that is used to calculate the cost and the factors that may increase or decrease these costs. We believe such information will help organisations make better decisions about how to allocate resources to minimize the financial consequences when the inevitable data breach strikes.

- **The unexpected and unplanned loss of customers following a data breach (churn rate)**

Programs that preserve customer trust and loyalty in advance of the breach will help reduce the number of lost business/customers. In this year's research, more organisations worldwide lost customers as a result of their data breaches. However, as shown, having a senior-level leader such as a chief privacy officer or chief information security officer who will be able to direct initiatives that improve customers' trust in how the organisation safeguards their personal information will reduce churn and the cost of the breach. Organisations that offer data breach victims breach identity protection in the aftermath of the breach are also more successful in reducing churn.

- **The size of the breach or the number of records lost or stolen**

It makes sense that the more records lost, the higher the cost of data breach. Therefore, data classification schema and retention programs are critical to having visibility into the sensitive and confidential information that is vulnerable to a breach and reducing the volume of such information.

- **The time it takes identify and contain a data breach**

The faster the data breach can be identified and contained, the lower the costs. In this year's study, organisations were able to reduce the days to identify the data breach from an average of approximately 201 in 2016 to 191 days and the average days to contain the data breach from 70 to 66 days. We attribute these improvements to investments in such enabling security technologies as security analytics, SIEM, enterprise wide encryption and threat intelligence sharing platforms.

In contrast, security complexity and the deployment of disruptive technologies can affect the time to detect and contain a data breach. Although some complexity in an IT security architecture is expected to deal with the many threats facing organisations, too much complexity can impact the ability to respond to data breaches. Disruptive technologies, access to cloud-based applications and data as well as the use of mobile devices (including BYOD and mobile apps) increase the complexity of dealing with IT security risks and data breaches. As shown in the research, cloud migration at the time of the data breach and mobile platforms were shown to increase the cost.

- **The detection and escalation of the data breach incident**

Detection and escalation costs include forensic and investigative activities, assessment and audit services, crisis team management and communications to executive management and board of directors. Investments in governance, risk management and compliance (GRC) programs that establish an internal framework for satisfying governance requirements, evaluating risk across the enterprise and tracking compliance with governance requirements can improve an organisation's ability to detect and escalate a data breach.

- **Post data breach costs, including the cost to notify victims**

These costs include help desk activities, inbound communications, special investigative activities, remediation, legal expenditures, product discounts, identity protection services and regulatory interventions. The United States had the highest notification costs.

The purchase of cyber and data breach insurance can help manage the financial consequences of the incident. As shown in this year's study, insurance protection and business continuity management reduced the cost of data breach following the discovery of the incident. In contrast, the rush to notify victims without understanding the scope of the breach, compliance failures and the engagement of consultants all increase post data breach costs. Expenditures to resolve lawsuits also increase post data breach costs.

- **An attack by a malicious insider or criminal is costlier than system glitches and negligence (human factor).**

Almost half of organisations represented in this research (47 percent) identified the root cause of the data breach as a malicious or criminal attack and the average cost was approximately $156. In contrast system glitches and human error or negligence averaged approximately $128 and $126, respectively. Factors that may decrease the cost are participation in threat sharing, use of security analytics and the recruitment and retention of knowledgeable personnel.

In conclusion, organisations in Australia, Germany, France and the United Kingdom were able to improve their ability to keep customers and, as a result, reduced the cost of data breach. Organisations in Australia, the United Kingdom and Germany also were able to limit the number of customer records lost or stolen and, as a result, had lower costs. Whereas, countries in the Middle East and the United States experienced a higher percentage of churn and had higher costs. Organisations in Brazil, India, the Middle East and South Africa had data breaches involving more lost or stolen records, which increased their costs. The individual country reports present in greater detail the cost components and factors that affected the cost.

The following are the most interesting findings and implications for organisations:

The per capita cost of data breach increases.[2] According to this year's benchmark findings, data breaches cost companies an average of 1,632 ZAR per compromised record, of which 774 ZAR are indirect costs, including abnormal turnover or churn of customers, and 809 ZAR are direct costs incurred to resolve the data breach. Last year's average per capita cost was 1,548 ZAR with an average indirect cost of 739 ZAR and an average direct cost of 858 ZAR.

The average total cost of data breach increases. The average total cost of data breach for the 21 companies represented in this research increased from 28.6 million ZAR in 2016 to 32.36 million ZAR in 2017. The largest cost component was lost business and the smallest cost component was data breach notification.

Certain industries have higher data breach costs. Financial, services and industrial companies had a per capita data breach cost substantially above the overall mean of 1,632 ZAR. Retail, public sector and media organisations had a per capita cost well below the overall mean value.

Malicious attacks and human error cause most data breaches. Forty-three percent of incidents involved a data theft (exfiltration) or criminal misuse and another 29 percent involved employee negligence or human error. System glitches and business process failures represented 28 percent of all data breaches.

Malicious attacks are most costly. Companies that experienced malicious attacks had a per capita data breach cost of 1,903 ZAR, which is significantly above the mean. In contrast, companies that experienced system glitches (1,425 ZAR) or employee negligence (1,432 ZAR) had per capita costs below the mean value.

Four new factors are added to this year's cost analysis. The following factors that influence data breach costs were added to this year's research: (1) compliance failures, (2) the extensive use of mobile platforms, (3) CPO appointment and (4) the use of security analytics. The appointment of a CPO and the use of security analytics decreased the cost of data breach by 20 ZAR and 41 ZAR, respectively. Whereas, data breaches caused by compliance failures and extensive use of mobile platforms, increased the per capita cost by 79 ZAR and 90 ZAR per compromised record, respectively.

The more records lost, the higher the cost of the data breach. In this year's study, the cost of data breach ranged from 24.9 million ZAR for data breaches involving 10,000 or fewer lost or stolen records to 39.1 million ZAR for the loss or theft of 25,001 to 50,000 records.

The more churn, the higher the cost of data breach. If companies lost 1 to 2 percent of their existing customers, the average cost of a breach could be 26.9 million ZAR, below the mean. When companies had a churn rate between 3 and 4 percent, the average cost could be $38.5 million ZAR, well above the mean.

Certain industries are more vulnerable to the loss of customers or churn. Financial, services and industrial organisations experienced relatively high abnormal churn and public sector and consumer product companies experienced a low abnormal churn rate

Detection and escalation costs increase significantly. Such costs typically include forensic and investigative activities, assessment and audit services, crisis team management, and communications to executive management and board of directors. Average detection and escalation costs increased from 9.50 million ZAR in 2016 to 11.60 million ZAR in 2017.

[2]Per capita cost is defined as the total cost of data breach divided by the size of the data breach in terms of the number of lost or stolen records.

Notification costs increase. Such costs typically include IT activities associated with the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, email bounce-backs and inbound communication set up. This year's average notification costs increased from 0.56 million ZAR in 2016 to $0.61 million ZAR in 2017.

Post data breach costs increase. These costs typically include help desk activities, inbound communications, special investigative activities, remediation activities, legal expenditures, product discounts, identity protection services and regulatory interventions. Average ex postee response cost increased from 7.99 million ZAR in 2016 to 8.07 million ZAR in 2017.

Lost business costs increase. Lost business costs include customer turnover, increased customer acquisition activities, reputation losses and diminished goodwill. Lost business costs increased from 10.55 million ZAR in 2016 to 12.08 million ZAR in 2017.

Indirect costs are higher than direct costs. The indirect cost of data breach includes costs related to the amount of time, effort and other organisational resources spent to resolve the breach. Average indirect costs were 774 ZAR, with an increase of 35 ZAR. Direct costs are the actual expense incurred to accomplish a given activity such as purchasing a technology or hiring a consultant. The average direct costs were 858 ZAR, with an increase of 49 ZAR.

The time to identify and contain data breaches impact costs. In this year's study, it took companies an average of 155 days to detect that an incident occurred and an average of 44 days to contain the incident. If the mean time to identify (MTTI) was less than 100 days, the average cost to identify the breach was 29.80 million ZAR. However, if the time to identify was greater than 100 days the cost rose significantly to 34.95 million ZAR. If the mean time to contain (MTTC) the breach was less than 30 days, the average cost was 28.44 million ZAR. If it took 30 days or longer, the cost significantly increased to 36.28 million ZAR.

Cost of Data Breach FAQs

What is a data breach? A breach is defined as an event in which an individual's name and a medical record and/or a financial record or debit card is potentially put at risk—either in electronic or paper format. In our study, we have identified three main causes of a data breach. These are a malicious or criminal attack, system glitch or human error. The costs of a data breach may vary according to the cause and safeguards in place at the time of the data breach.

What is a compromised record? We define a record as information that identifies the natural person (individual) whose information has been lost or stolen in a data breach. Examples include a retail company's database with an individual's name associated with credit card information and other personally identifiable information or a health insurer's record of the policyholder with physician and payment information. In this year's study, the average cost to the organisation if one of these records is lost or stolen is 1,632 ZAR.

How do you collect the data? Ponemon Institute researchers collected in-depth qualitative data through interviews conducted over a 10-month period. Recruiting organisations for the 2017 study began in February 2016 and interviews were completed in March 2017. In each of the 21 participating organisations, we spoke with IT, compliance and information security practitioners who were knowledgeable about their organisation's data breach and the costs associated with resolving the breach. For privacy purposes, we do not collect any organisation-specific information.

How do you calculate the cost of data breach? To calculate the average cost of data breach, we collected both the direct and indirect expenses the organisation incurs. Direct expenses include engaging forensic experts, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and services. Indirect costs include in-house investigations and communications as well as the extrapolated value of customer loss resulting from turnover or diminished customer acquisition rates.

How does benchmark research differ from survey research? The unit of analysis in the *Cost of Data Breach Study* is the organisation. In survey research, the unit of analysis is the individual. We recruited 21 organisations to participate in this study. Data breaches ranged from a low of 2,400 compromised to a high of 76,900 compromised records.

Can the average cost of data breach be used to calculate the financial consequences of a mega breach such as one involving millions of lost or stolen records? The average cost of a data breach in our research does not apply to catastrophic or mega data breaches because these are not typical of the breaches most organisations experience. To be representative of the population of South African organisations and draw conclusions from the research that can be useful in understanding costs when protected information is lost or stolen, we do not include data breaches of more than 100,000 compromised records in our analysis.

Do you track the same organisations each year? Each annual study involves a different sample of companies. In other words, we do not track the same sample of companies over time. To be consistent, we recruit and match companies with similar characteristics such as the company's industry, headcount, geographic footprint and size of data breach. Since starting this research, we have studied the data breaches of 40 organisations located in South Africa.

Part 2. Key Findings

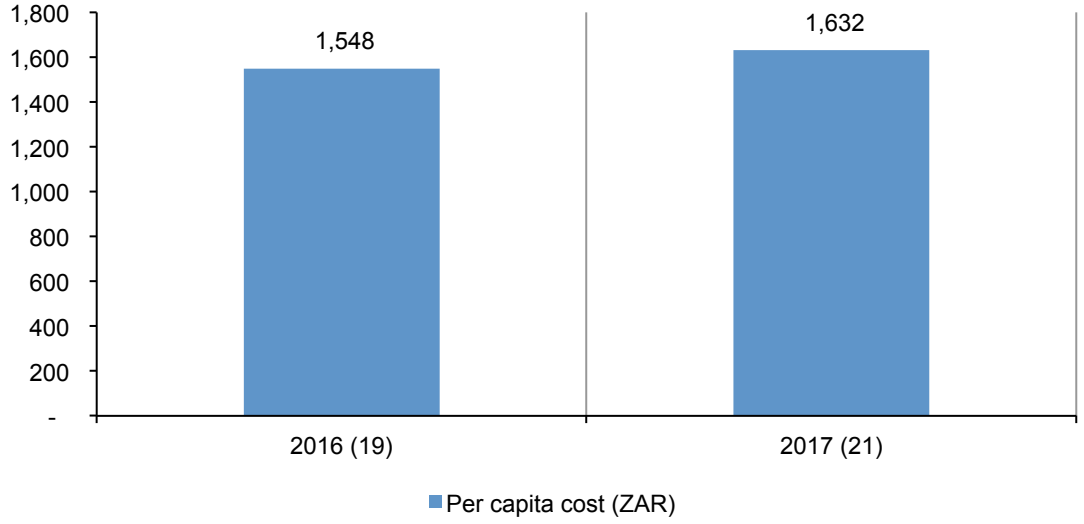
In this section we provide the detailed findings of this research. Topics are presented in the following order:

- Trends in the cost of data breach
- The root causes of a data breach
- Factors that influence the cost of data breach
- Trends in the cost components of a data breach
- The time to identify and contain data breaches affects cost
- Trends in practices to reduce the risk and consequences of a data breach

Trends in the cost of data breach

The per capita cost of data breach increases. Figure 1 reports the average per capita cost of data breach.[3] According to this year's benchmark findings, data breaches cost companies an average of 1,632 ZAR per compromised record, of which 774 ZAR pertains to indirect costs including abnormal turnover or churn of customers and 858 ZAR pertains to direct costs incurred to resolve the data breach. Last year's average per capita cost was 1,548 ZAR with an average indirect cost of 739 ZAR and an average direct cost of 858 ZAR.

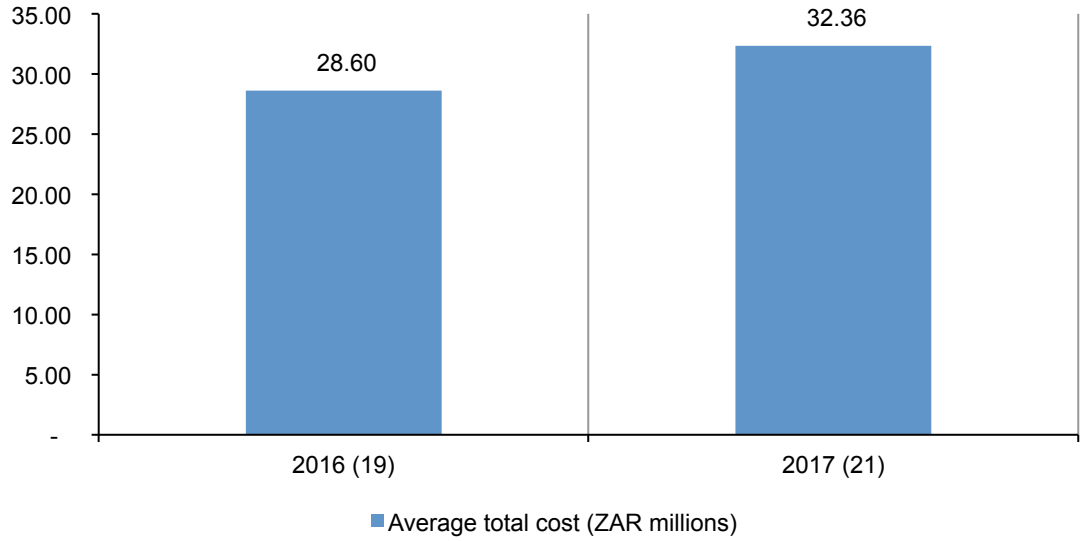
Figure 1. The average per capita cost of data breach over the past two years
Bracketed number defines the benchmark sample size
Measured in South African Rand (ZAR)



[3]Per capita cost is defined as the total cost of data breach divided by the size of the data breach in terms of the number of lost or stolen records.

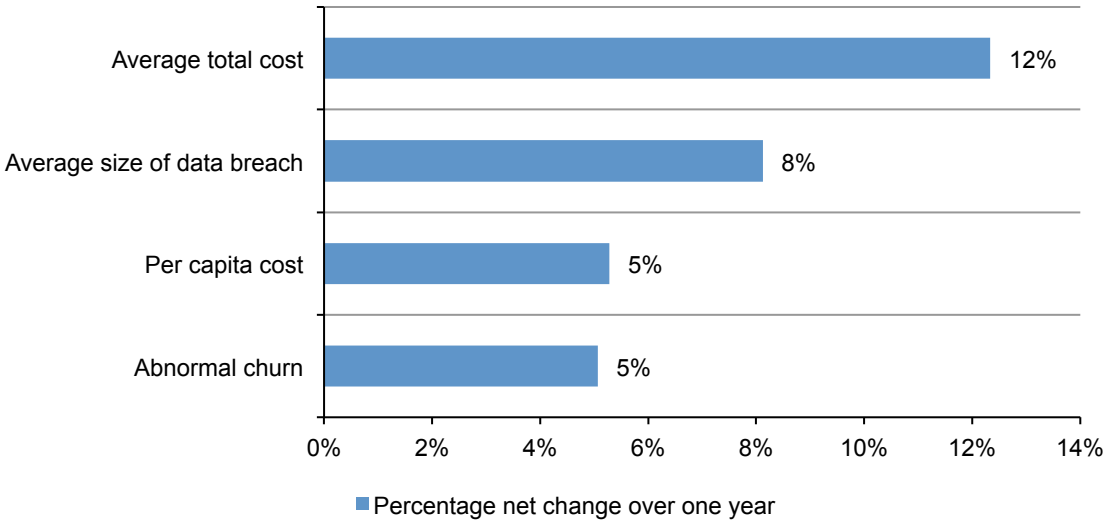
The total average organisational cost of data breach increases. The total cost of data breach increased from 28.60 million ZAR in 2016 to 32.36 million ZAR in 2017.

Figure 2. Average total organisational cost of data breach over the past two years
Measured in South African Rand (ZAR)



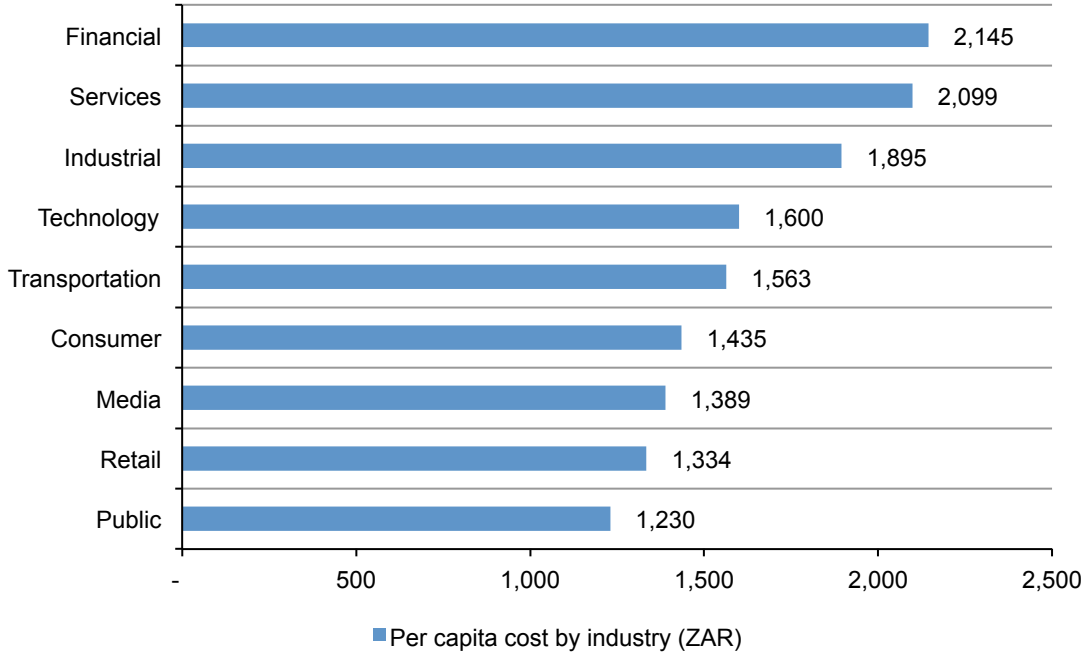
Measures reveal why the cost of data breach increased. Figure 3 reports the percentage net change in four key metrics over one year. As can be seen, the per capita cost increased 5 percent, the average total cost increased 12 percent, abnormal churn, which is defined as the greater than expected loss of customers in the normal course of business, increased 5 percent and the average size of data breach (number of records lost or stolen) increased 8 percent.

Figure 3. Cost of data breach measures
Net change defined as the difference between the 2017 and 2016 results



Certain industries have higher data breach costs. Figure 4 reports the per capita cost for nine industries. Although a small sample size prevents us from generalising industry cost differences, financial, services and industrial companies had a per capita data breach cost substantially above the overall mean of 1,632 ZAR. Retail and public sector had a per capita cost well below the overall mean value.

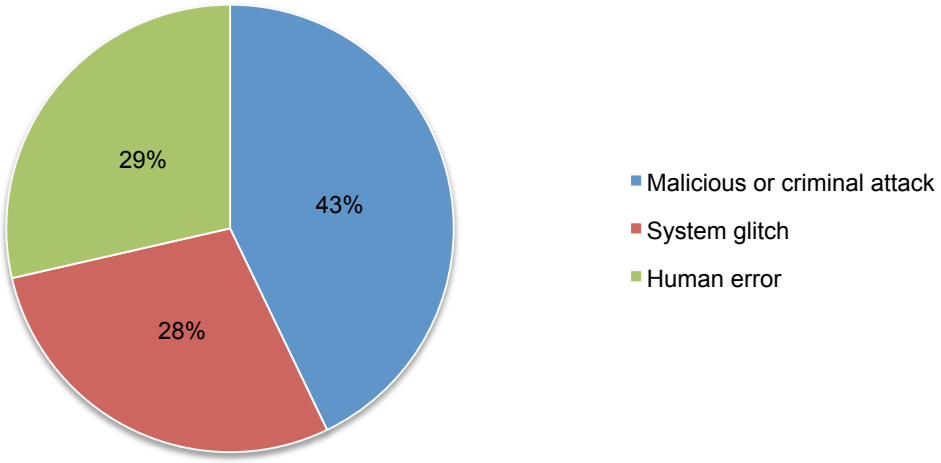
Figure 4. Per capita cost by industry
Measured in South African Rand (ZAR)



The root causes of a data breach

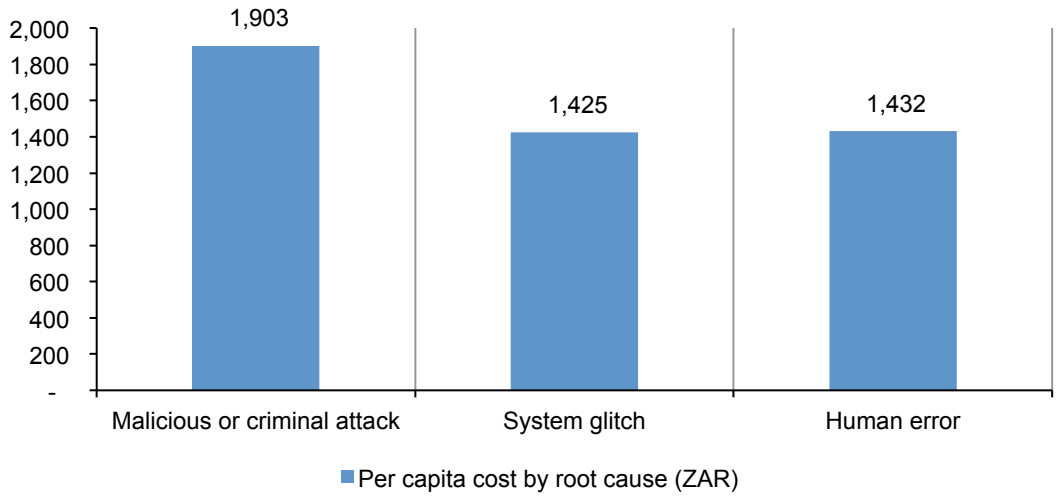
Malicious and criminal attacks cause most data breaches.[4] Figure 5 provides the three main root causes of data breach for all 21 organisations. Forty-three percent of incidents involved a data theft (exfiltration) or criminal misuse and another 29 percent of incidents involved employee negligence or human error.[5] System glitch or business process failure was the root cause of 28 percent of all data breaches.

Figure 5. Distribution of the benchmark sample by root cause of the data breach



Malicious attacks are the costliest. Figure 6 reports the per capita cost of data breach for the three root causes. Companies that experienced malicious attacks had a per capita data breach cost of 1,903 ZAR. In contrast, companies that experienced system glitches (1,425 ZAR) or employee negligence (1,432 ZAR) had per capita costs below the mean.

Figure 6. Per capita cost for three root causes of the data breach
Measured in South African Rand (ZAR)



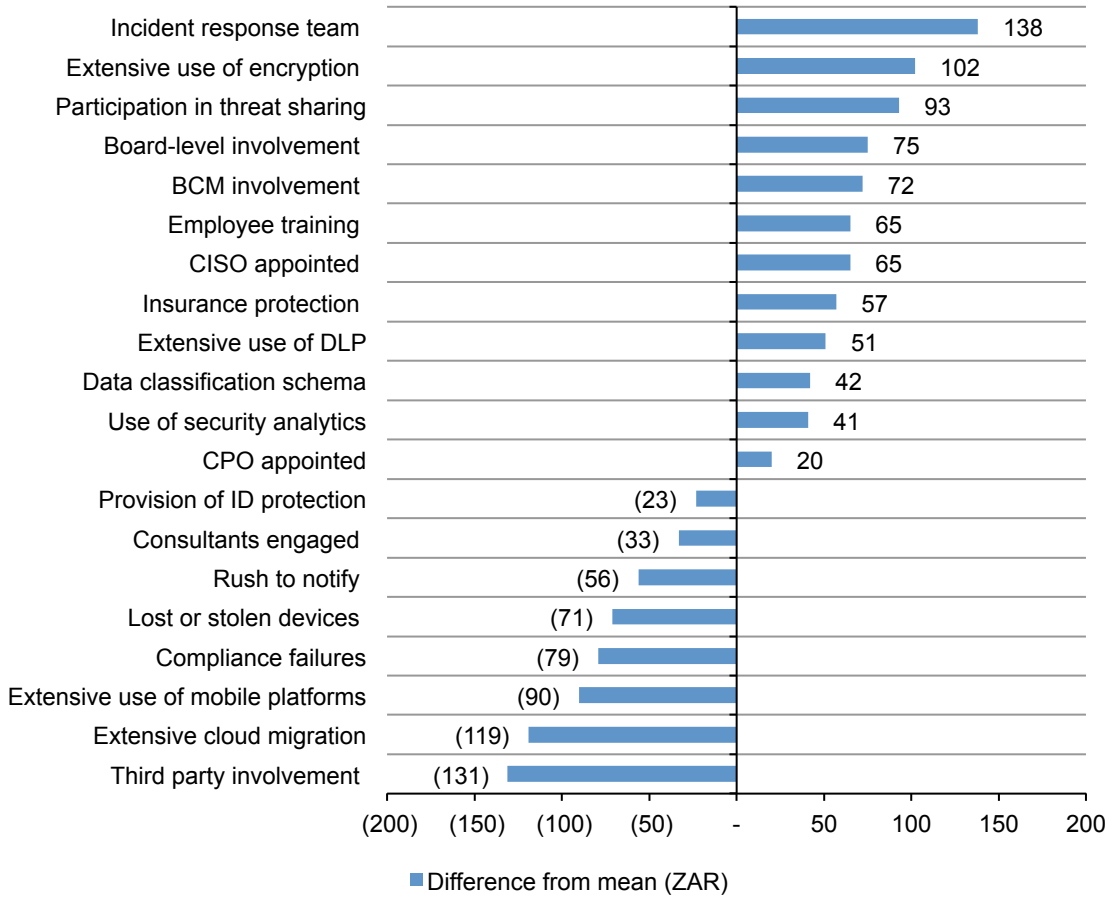
[4]Negligent insiders are individuals who cause a data breach because of their carelessness, as determined in a post data breach investigation. Hackers or criminal insiders (employees, contractors or other third parties) cause malicious attacks
[5]The most common types of malicious or criminal attacks include malware infections, criminal insiders, phishing/social engineering and SQL injection.

Factors that influence the cost of data breach

Four new factors are added to this year's cost analysis. As shown in Figure 7, the following factors that influence data breach costs were added to this year's research: (1) compliance failures, (2) the extensive use of mobile platforms, (3) CPO appointment and (4) the use of security analytics. The appointment of a CPO and the use of security analytics decreased the cost of data breach by 20 ZAR and 41 ZAR, respectively.

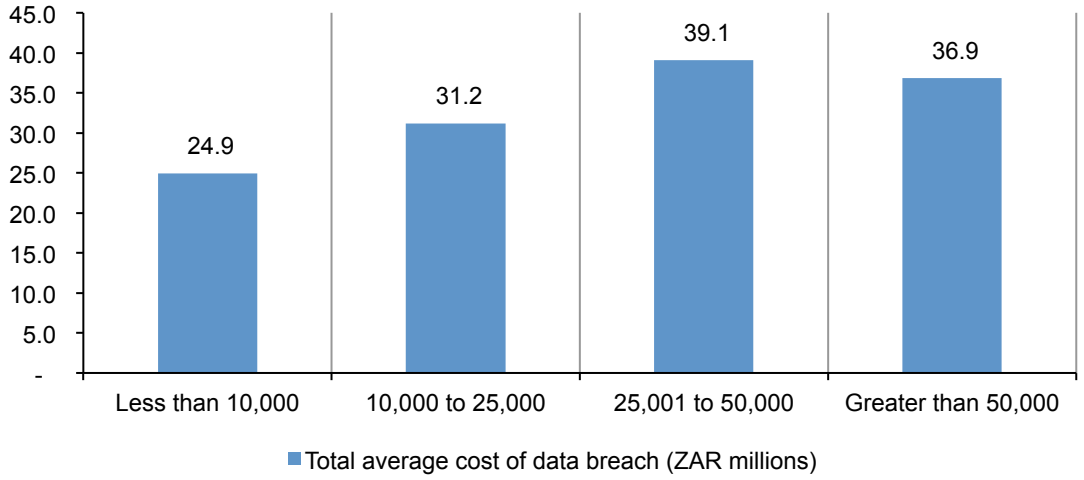
To illustrate how these factors may affect the cost of data breach, the availability of an incident response team reduced the per capita cost to 1,494 ZAR (1,632 ZAR-138 ZAR). In contrast, a third party error increased the cost by to 1,763 ZAR (1,632 ZAR+131 ZAR).

Figure 7. Impact of 20 factors on the per capita cost of data breach
Measured in South African Rand (ZAR)



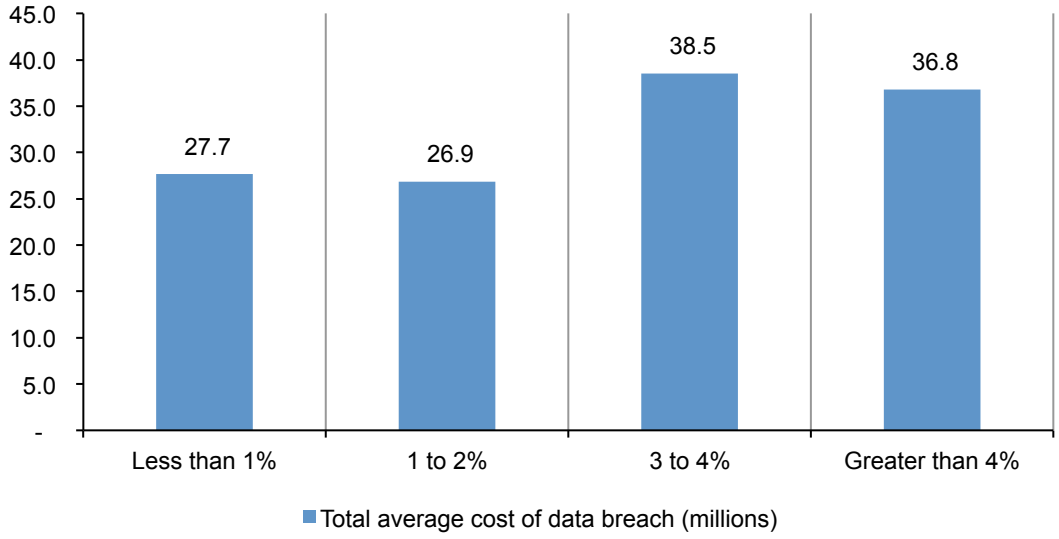
The more records lost, the higher the cost of the data breach. Figure 8 shows the relationship between the total cost of a data breach and the size of the incident for 21 benchmarked companies in ascending order by the size of the breach incident. The cost ranged from 24.9 million ZAR for data breaches involving 10,000 or fewer to 39.1 million ZAR for the loss or theft between 25,001 and 50,000 records.

Figure 8. Average total cost of data breach by size
Measured in South African Rand (ZAR millions)



The more churn, the higher the cost of data breach. Figure 9 reports the distribution of per capita data breach costs in ascending rate of abnormal churn. If companies lost 1 to 2 percent of their existing customers, the average cost of a breach was 26.9 million ZAR, well below the mean value. When companies had a churn rate between 3 and 4 percent, the average cost was 38.5 million ZAR.

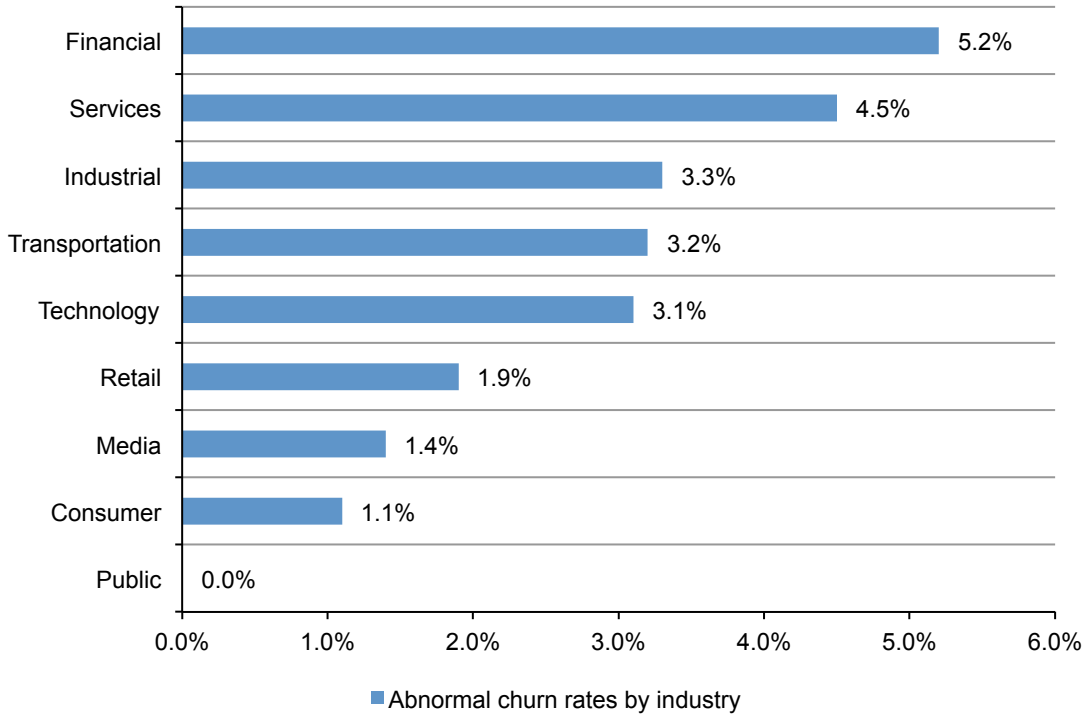
Figure 9. Average total cost of data breach by abnormal churn rate
Measured in South African Rand (ZAR millions)



Certain industries are more vulnerable to churn. Figure 10 reports the abnormal churn rate for nine industries. Although a small sample size prevents us from generalising the effect of industry on abnormal churn rates, our results show marked variation. Financial, services and industrial organisations experienced relatively high abnormal churn. In contrast, public sector and consumer product companies experienced a relatively low abnormal churn rate.[6]

The key takeaway is that industries with the highest churn rates could significantly reduce the cost of data breach by emphasising customer retention and activities to preserve reputation and brand value.

Figure 10. Abnormal churn rates by industry

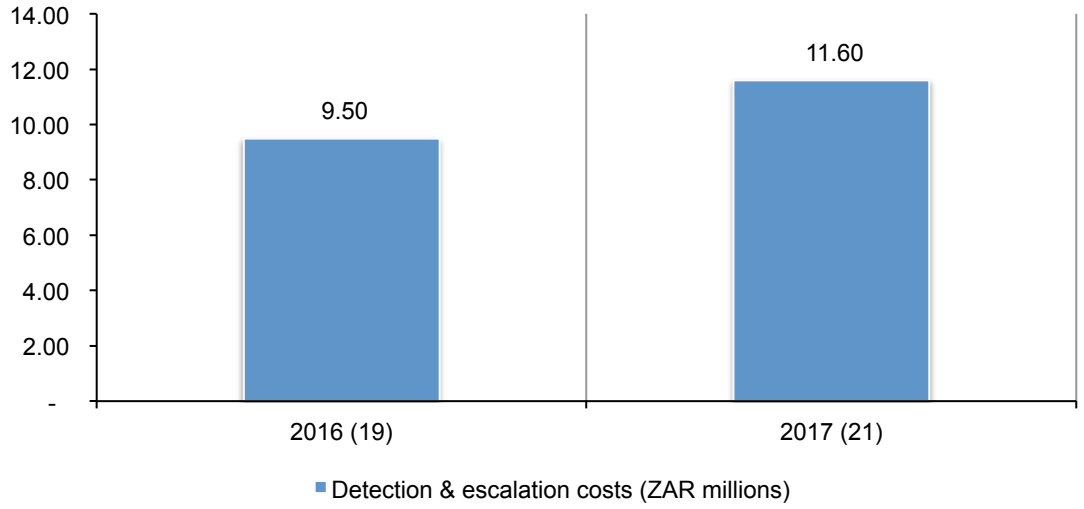


[6]Public sector organisations utilise a different churn framework given that customers of government organisations typically do not have an alternative choice.

Trends in the cost components of a data breach

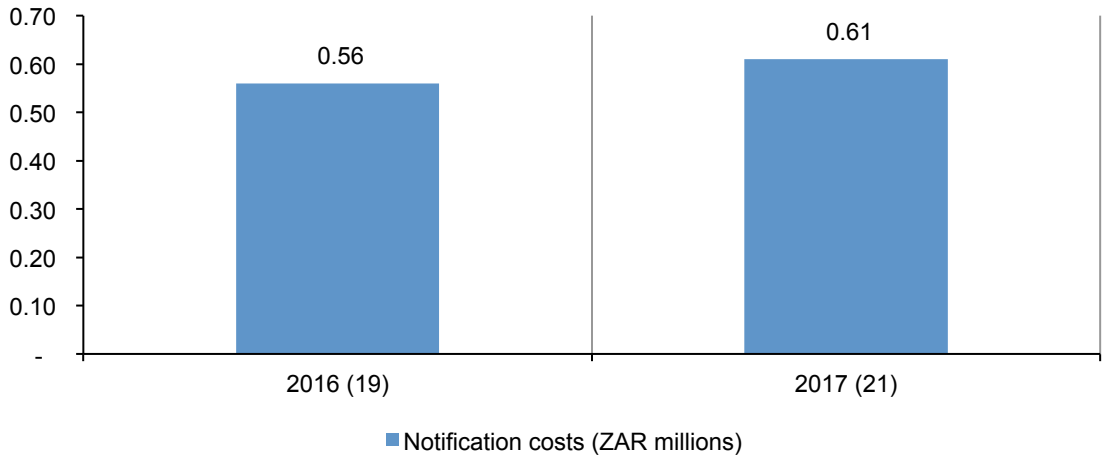
Detection and escalation costs increase significantly. Figure 11 shows the two-year trend for costs relating to the detection and escalation of the data breach incident. Such costs typically include forensic and investigative activities, assessment and audit services, crisis team management, and communications to executive management and boards of directors. Average detection and escalation costs increased from 9.50 million ZAR in 2016 to 11.60 million ZAR in 2017.

Figure 11. Average detection and escalation costs over the past two years
Measured in South African Rand (ZAR millions)



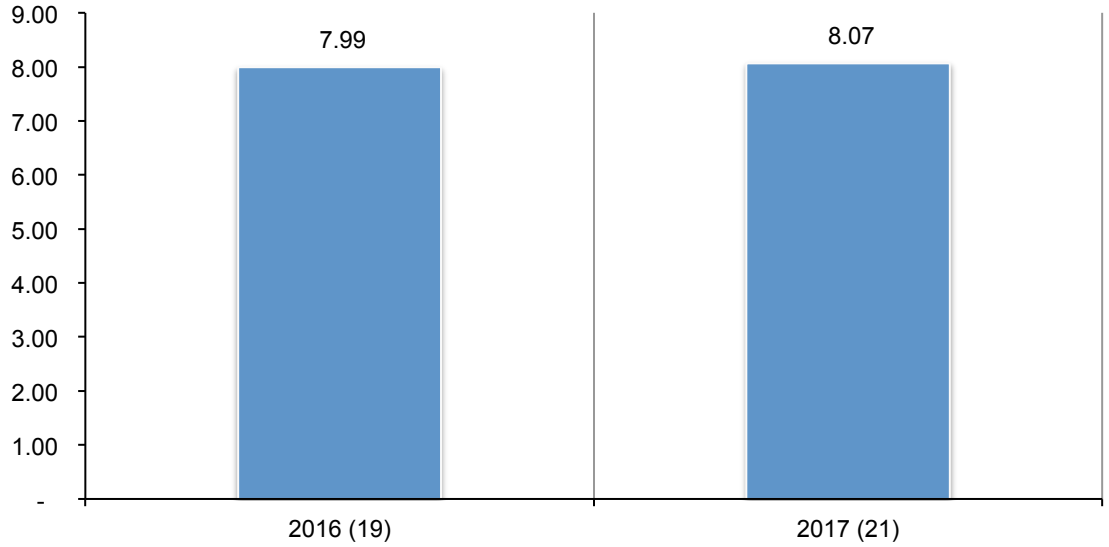
Notification costs increase. Figure 12 reports cost trends associated with notification activities. Such costs typically include IT activities associated with the creation of contact databases, determination of all regulatory requirements, engagement of outside experts, postal expenditures, email bounce-backs and inbound communication set-up. This year's average notification increased from 0.56 million ZAR in 2016 to 0.61 million ZAR in 2017.

Figure 12. Average notification costs over two years
Measured in South African Rand (ZAR millions)



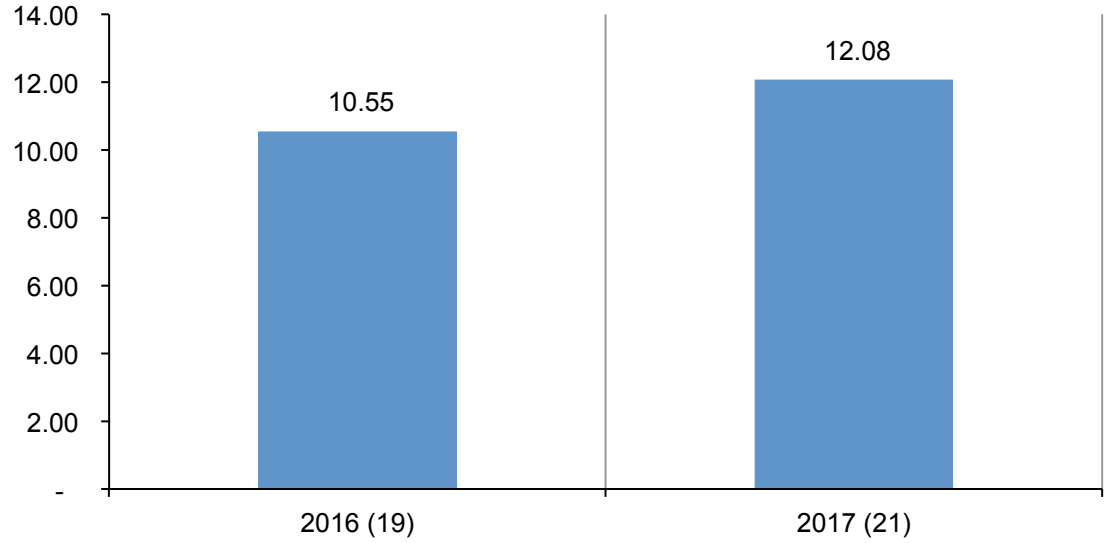
Post data breach costs increase. Figure 13 shows the distribution of costs associated with ex-poste (after-the-fact) activities. Such costs typically include help desk activities, inbound communications, special investigative activities, remediation activities, legal expenditures, product discounts, identity protection services and regulatory interventions. Average ex-post response cost increased from 7.99 million ZAR in 2016 to 8.07 million ZAR in 2017.

Figure 13. Average ex poste response costs over the past two years
Ex poste costs measured in South African Rand (ZAR millions)



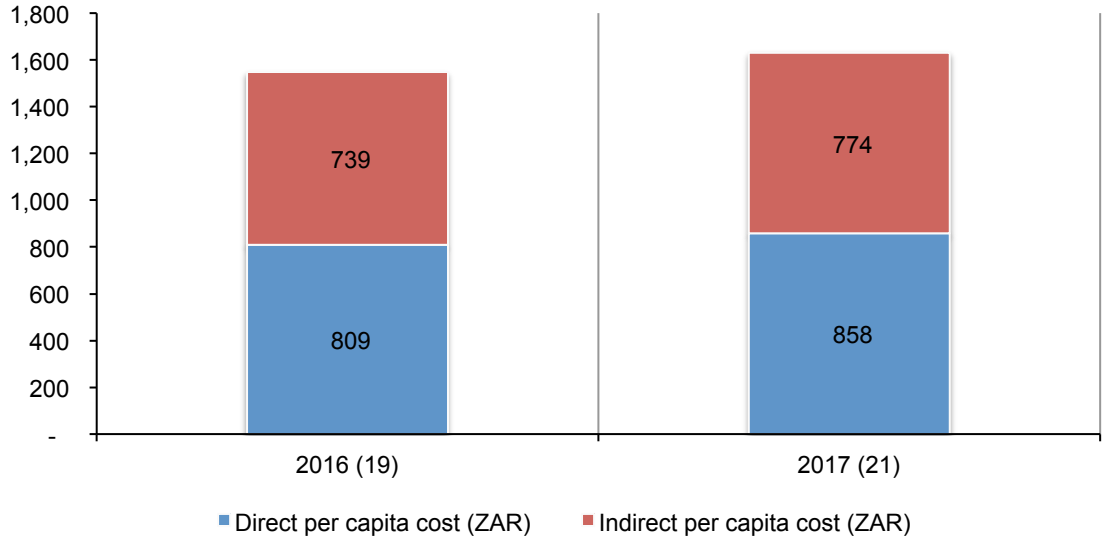
Lost business costs increase. Figure 14 reports lost business costs associated with data breach incidents over two years. The cost category typically includes customer turnover, increased customer acquisition activities, reputation losses and diminished goodwill. As can be seen below, lost business costs increased from 10.55 million ZAR in 2016 to 12.08 million ZAR in 2017.

Figure 14. Average lost business costs over the past two years
Lost business costs measured in South African Rand (ZAR millions)



Both direct and indirect costs increase. Figure 15 reports the direct and indirect cost components of a data breach on a per capita basis. The indirect cost of a data breach includes costs related to the amount of time, effort and other organisational resources spent to resolve the breach. Average indirect costs were 774 ZAR, with an increase of 35 ZAR. Direct costs are the actual expense incurred to accomplish a given activity such as purchasing a technology or hiring a consultant. The average direct costs increased 49 ZAR to 858 ZAR.

Figure 15. Direct and indirect per capita data breach costs
Measured in South African Rand (ZAR)



The time to identify and contain data breaches affects cost

The faster to identify and contain a data breach the lower the costs. MTTI and MTTC metrics are used to determine the effectiveness of an organisation's incident response and containment processes. MTTI measures the time it takes to detect an incident and MTTC measures the time it takes to respond and contain a data breach. As shown in Figure 16, it took an average of 155 days to detect an incident and 44 days to contain the incident.

Figure 16. Days to identify and contain a data breach

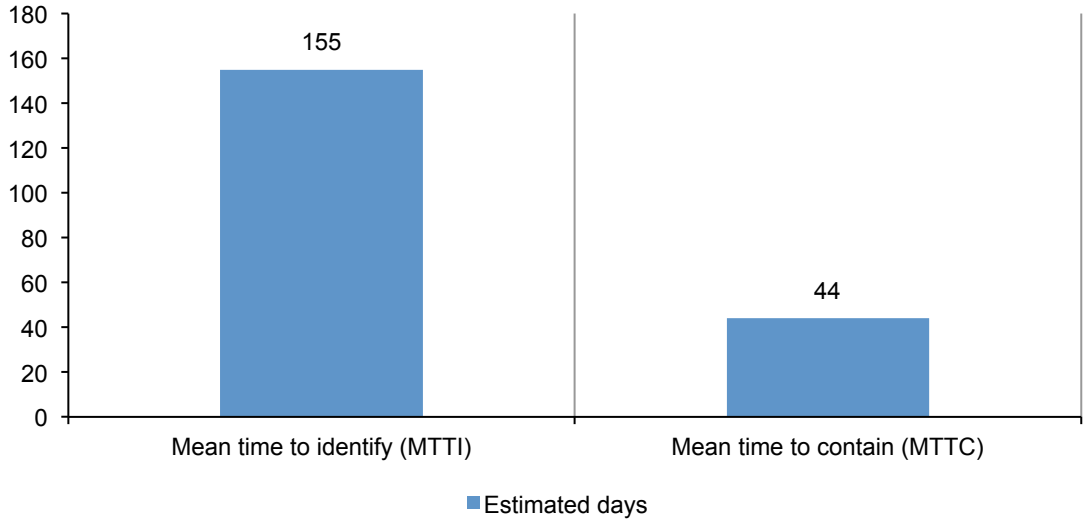
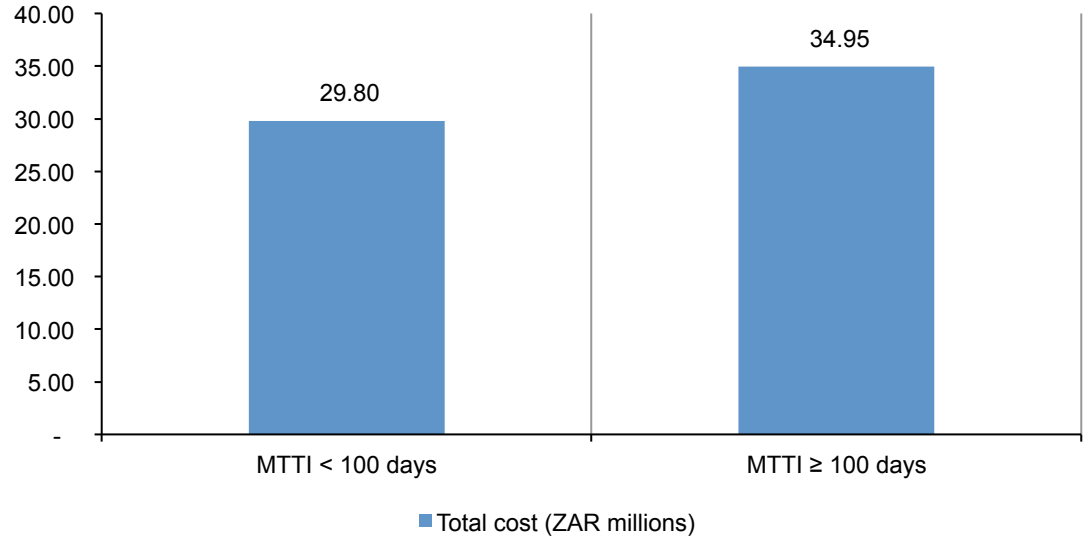


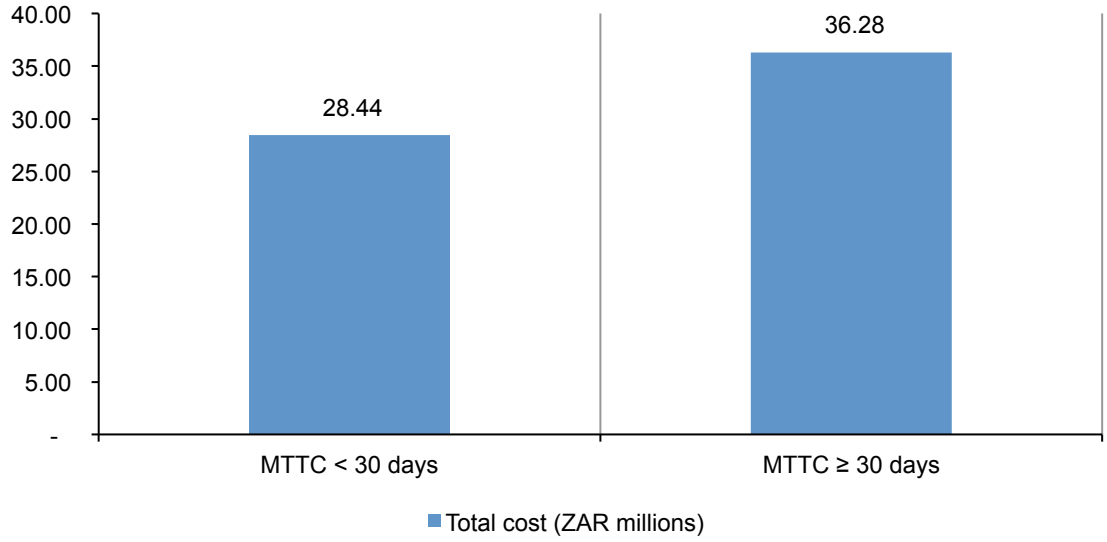
Figure 17 highlights the importance of having an incident response plan in place. If MTTI was less than 100 days, the average cost to resolve the data breach was 29.80 million ZAR. However, if MTTI was greater than 100 days, the average cost rose significantly to 34.95 million ZAR.

Figure 17. Time to identify and average total cost
Measured in South African Rand (ZAR millions)



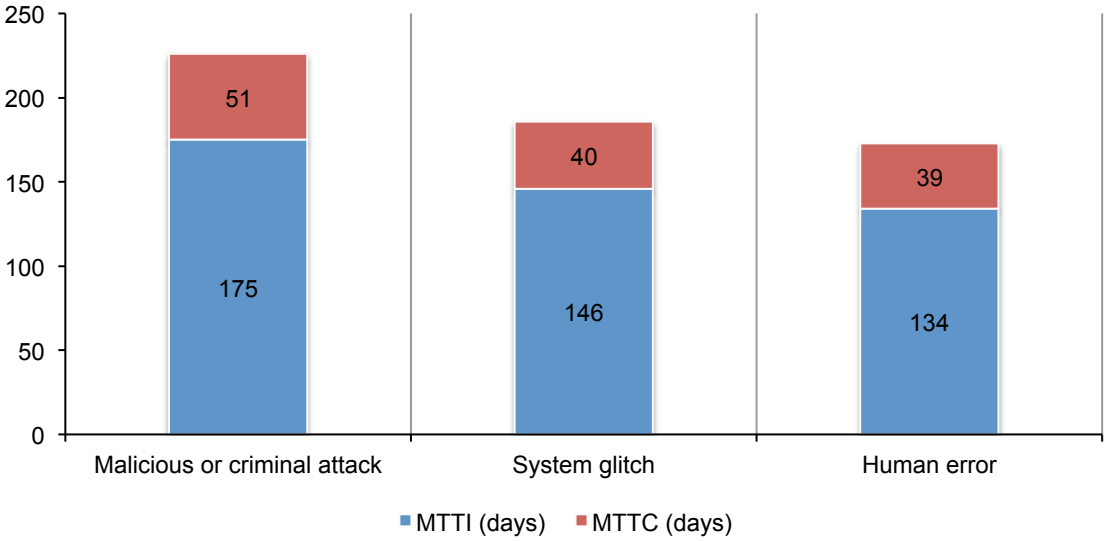
As shown in Figure 18, if the time it took to contain the breach was less than 30 days, the average cost of data breach was 28.44 million ZAR, if it took 30 days or longer to contain the breach, the cost increased to 36.28 million ZAR.

Figure 18. Days to contain the data breach and average total cost
Measured in South African Rand (ZAR millions)



The most difficult and time-consuming incident to detect and contain, as shown in Figure 19, is the malicious or criminal act (226 days). Data breaches caused by human error (173 days) and system glitches (186 days) take less time to detect and contain.

Figure 19. Days to identify and contain the data breach by root cause



Trends in practices to reduce the risk and consequences of a data breach

Investment in improving data protection practices is important to minimise the occurrence and financial consequences of a data breach. In this study, incident response teams and plans, the extensive use of encryption, threat intelligence sharing, employee training programs and board-level involvement decreased the per capita costs of data breaches.

In addition to measuring specific cost activities relating to the loss or theft of personal information, we report in Table 1 the preventive measures implemented by companies after the data breach. The most popular measures or steps taken were: training and awareness programs (60 percent), additional manual procedures and controls (49 percent), expanded use of encryption (45 percent) and security certification or audit (52 percent).

Table 1. Preventive measures and controls implemented after the data breach	2016	2017
Training and awareness programs	57%	60%
Security certification or audit	43%	52%
Additional manual procedures & controls	52%	49%
Expanded use of encryption	43%	45%
Identity and access management solutions	33%	40%
Security intelligence systems	33%	37%
Endpoint security solutions	29%	33%
Data loss prevention (DLP) solutions	19%	21%
Strengthening of perimeter controls	19%	18%
Other system control practices	19%	16%

Please note that a company may be implementing more than one preventive measure.

Table 2 reports 11 general cost categories on a percentage basis. The two highest cost categories are lost customer business (37 percent) and investigations and forensics (25 percent).

Table 2. Percentage data breach cost categories over two years	2016	2017
Investigations & forensics	23%	25%
Audit and consulting services	10%	10%
Outbound contact costs	5%	5%
Inbound contact costs	2%	1%
Public relations/communications	2%	0%
Legal services – defense	4%	3%
Legal services – compliance	6%	5%
Free or discounted services	3%	1%
Identity protection services	2%	2%
Lost customer business	34%	37%
Customer acquisition cost	9%	11%
Total	100%	100%

Part 3. How We Calculate the Cost of Data Breach

To calculate the cost of data breach, we use a costing methodology called activity-based costing (ABC). This methodology identifies activities and assigns a cost according to actual use. Companies participating in this benchmark research are asked to estimate the cost for all the activities in which they engage to resolve a data breach.

Typical activities for discovery and the immediate response to the data breach include the following:

- Conducting investigations and forensics to determine the root cause of the data breach
- Determining the probable victims of the data breach
- Organising the incident response team
- Conducting communication and public relations outreach
- Preparing notice documents and other required disclosures to data breach victims and regulators
- Implementing call centre procedures and specialised training

The following are typical activities conducted in the aftermath of discovery:

- Audit and consulting services
- Legal services for defence
- Legal services for compliance
- Free or discounted services offered to victims of the breach
- Identity protection services
- Lost customer business based on calculating customer churn or turnover
- Customer acquisition and loyalty program costs

Once the company estimates a cost range for these activities, we categorize the costs as direct, indirect and opportunity, as defined below:

- *Direct cost* – the direct expense outlay to accomplish a given activity.
- *Indirect cost* – the amount of time, effort and other organisational resources spent, but not as a direct cash outlay.
- *Opportunity cost* – the cost resulting from lost business opportunities as a consequence of negative reputation effects after the breach has been reported to victims (and publicly revealed to the media).

Our study also looks at the core process-related activities that drive a range of expenditures associated with an organisation's data breach detection, response, containment and remediation. The costs for each activity are presented in the Key Findings section (Part 2). The four cost centres are as follows:

- Detection or discovery: Activities that enable a company to reasonably detect the breach of personal data either at risk (in storage) or in motion.
- Escalation: Activities necessary to report the breach of protected information to appropriate personnel within a specified time period.
- Notification: Activities that enable the company to notify data subjects with a letter, outbound telephone call, email or general notice that personal information was lost or stolen.
- Post data breach: Activities to help victims of a breach communicate with the company to ask additional questions or obtain recommendations in order to minimise potential harm. Post data breach activities also include credit report monitoring or the reissuing of a new account (or credit card).

In addition to the above process-related activities, most companies experience opportunity costs associated with the breach incident, resulting from present and future customers' diminished trust or confidence. Accordingly, Ponemon Institute's research shows that the negative publicity associated with a data breach incident causes reputation effects that may result in abnormal turnover or churn rates and a diminished rate for new customer acquisitions.

To extrapolate these opportunity costs, we use a cost estimation method that relies on the "lifetime value" of an average customer as defined for each participating organisation.

- Turnover of existing customers: The estimated number of customers who will most likely terminate their relationship as a result of the breach incident. The incremental loss is abnormal turnover attributable to the breach incident. This number is an annual percentage, which is based on estimates provided by management during the benchmark interview process.[7]

- Diminished customer acquisition: The estimated number of target customers who will not have a relationship with the organisation as a consequence of the breach. This number is provided as an annual percentage.

We acknowledge that the loss of non-customer data, such as employee records, may not impact an organisation's churn or turnover.[8] In these cases, we expect the business cost category to be lower when data breaches do not involve customer or consumer data (including transactional payment information).

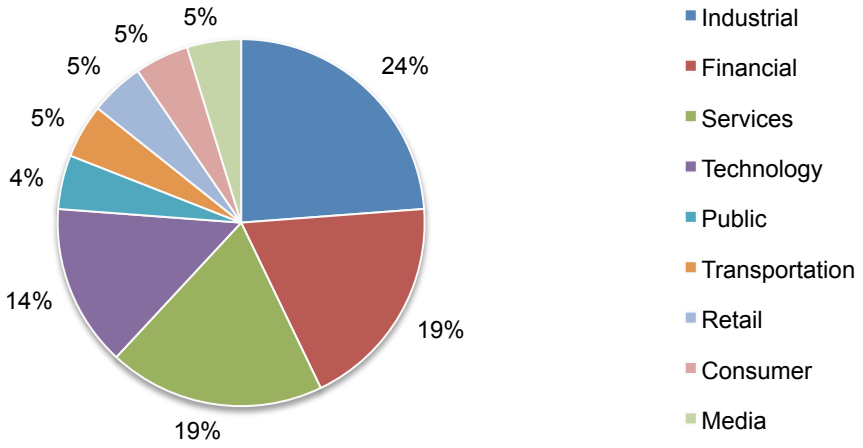
[7] In several instances, turnover is partial, as in the cases of breach victims continued their relationship with the breached organisation, but the volume of customer activity actually declines. This partial decline is especially salient in certain industries – such as financial services or public sector entities for which termination is costly or economically infeasible.

[8] In this study, we consider citizen, patient and student information to be customer data.

Part 4. Organisational characteristics and benchmark methods

Figure 20 shows the distribution of benchmark organisations by their primary industry classification. In this year's study, nine industries were represented. The two largest sectors were industrial and financial services, which includes banks, insurance, investment management and payment processors.

Figure 20. Distribution of the benchmark sample by industry segment



All participating organisations experienced one or more data breach incidents sometime over the past year. Our benchmark instrument captured descriptive information from IT, compliance and information security practitioners about the full cost impact of a breach involving the loss or theft of customer or consumer information. It also required these practitioners to estimate opportunity costs associated with program activities.

Estimated data breach cost components were captured on a rating form. In most cases, the researcher conducted follow-up interviews to obtain additional facts, including estimated abnormal churn rates that resulted from the company's most recent breach event involving 1,000 or more compromised records.[9]

[9]Our sampling criteria only included companies experiencing a data breach between 1,000 and 100,000 lost or stolen records sometime during the past 12 months. We excluded catastrophic data breach incidents to avoid skewing overall sample findings.

Data collection methods did not include actual accounting information, but instead relied on numerical estimation based on the knowledge and experience of each participant. The benchmark instrument required individuals to rate direct cost estimates for each cost category by marking a range variable defined in the following number line format.

How to use the number line: The number line provided under each data breach cost category is one way to obtain your best estimate for the sum of cash outlays, labour and overhead incurred. Please mark only one point somewhere between the lower and upper limits set above. You can reset the lower and upper limits of the number line at any time during the interview process.

Post your estimate of direct costs here for [presented cost category]

LL	_____|_____	UL

The numerical value obtained from the number line rather than a point estimate for each cost category presented preserved confidentiality and ensured a higher response rate. The benchmark instrument also required practitioners to provide a second estimate for indirect and opportunity costs, separately.

To keep the benchmarking process to a manageable size, we carefully limited items to only those cost activity centres that we considered crucial to data breach cost measurement. Based upon discussions with learned experts, the final set of items included a fixed set of cost activities. Upon collection of the benchmark information, each instrument was re-examined carefully for consistency and completeness.

For purposes of complete confidentiality, the benchmark instrument did not capture any company-specific information. Subject materials contained no tracking codes or other methods that could link responses to participating companies.

The scope of data breach cost items contained within our benchmark instrument was limited to known cost categories that applied to a broad set of business operations that handle personal information. We believed that a study focused on business process – and not data protection or privacy compliance activities – would yield better quality results.

Part 5. Limitations

Our study utilises a confidential and proprietary benchmark method that has been successfully deployed in earlier research. However, inherent limitations with this benchmark research need to be carefully considered before drawing conclusions from the findings.

- Non-statistical results: Our study draws upon a representative, non-statistical sample of South African organisations that experienced a breach involving the loss or theft of customer or consumer records during the past 12 months. Statistical inferences, margins of error and confidence intervals cannot be applied to the data given that our sampling methods are not scientific.

- Non-response: The current findings are based on a small representative sample of benchmarks. Twenty-one companies completed the benchmark process. Non-response bias was not tested so it is possible that companies that did not participate are substantially different in terms of underlying data breach cost.

- Sampling-frame bias: Because our sampling frame is judgmental, the quality of the results is influenced by the degree to which the frame is representative of the population of companies being studied. We believe that the current sampling frame is biased toward companies with more mature privacy or information security programs.

- Company-specific information: The benchmark information is sensitive and confidential. Thus, the current instrument does not capture company-identifying information. It also allows individuals to use categorical response variables to disclose demographic information about the company and industry category.

- Unmeasured factors: To keep the interview script concise and focused, we omitted other important variables from our analyses such as leading trends and organisational characteristics. The extent to which omitted variables might explain benchmark results cannot be determined.

- Extrapolated cost results: The quality of benchmark research is based on the integrity of confidential responses that the respondents in participating companies provided. Although certain checks and balances can be incorporated into the benchmark process, the possibility always exists that respondents did not provide accurate or truthful responses. In addition, the use of cost extrapolation methods rather than actual cost data may inadvertently introduce bias and inaccuracies.

If you have questions or comments about this research report or would like to obtain additional copies of the document (including permission to quote or reuse this report), please contact by letter, phone call or email the following:

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City, Michigan 49686 USA
1.800.887.3118
research@ponemon.org

Complete copies of all country reports are available at **www.ibm.com/security/data-breach**

Ponemon Institute LLC
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.