IBM & Ponemon Institute: Cost of a Data Breach Dropped 5 Percent in Australia in 2017 Study

Sydney - 21 Jun 2017: Today IBM announced the Australian results of the global 2017 Ponemon Cost of Data Breach report. The report highlights some interesting challenges for organisations in Australia. Currently Australian organisations on average are taking more than 175 days to detect an incident. From February 2018, The Data Privacy Act will require organisations to report data breaches within 30 days to the Privacy Commissioner and their customers. Technologies such as cognitive and AI can provide faster, more cost-effective incident identification, which will speed the customer response and reduce churn.

Key Australian Findings

Cost are Down

The average costs of a data breach for an Australian organisation has fallen 5% YOY to AUD$2.51 million, down from AUD$2.64 million. Globally, the average decreased by 10%

The average cost per lost or stolen record for Australian organisations was AUD$139 - a 2.1% decrease

Lost business costs (turnover of customers, increased acquisition activities, reputation losses and diminished goodwill) decreased from AUD$0.84 million to AUD$0.79 million this year.

Reasons for decreasing costs:

- Reduction in the number of stolen or lost records - a decrease of 5.8%
- Improvements in organisations' ability to retain customers following a data breach. Abnormal churn (the greater-than-expected loss of customers) decreased by 5.3%

Certain industries have higher data breach costs:

- Financial services, services and technology companies tend to have higher per capita cost than the average cost of AUD$139. For example, financial services can cost as much as AUD$232
- Companies in public sector, transportation and retail had a per capita cost significantly below, and experience lower rates of churn

Breach Cause and Impact

Root cause of data breach:

- 48% driven from malicious or criminal attacks with the cost of remediation at AUD$154
- 28% of incidents involved negligent employee or contractors, at AUD$130 cost
- 24% due to system glitches, at AUD$121

On average, Australian organisations took more than 5 months, 175 days to detect that an incident occurred, 16 days quicker than the global average.

Organisation took 67 days to contain this incident, one day slower than the global average.

Speed of response impacts cost significantly:

- The faster companies can identify and contain the breach, the lower the breach costs. If the mean time to identify (MTTI) was less than 100 days, organisations could save 35% (AUD$1.96 million v AUD$3.05 million).

Taking Action

The most profitable investment that organisations made to reduce costs a data breach include:

- Extensive use of encryption
- Having an incident response team in place
- Employee training
- CISO appointed
- Participation in threat sharing

Organisations in Australia and globally can consider the following to reduce their costs of data breach:

- Investments in governance, risk management and compliance (GRC) programs.
- Investment in enabling security technologies. These include security analytics, SIEM, enterprise wide encryption and threat intelligence sharing platforms.
- Recruitment and retention of knowledgeable personnel.

IBM & Ponemon Institute: Cost of a Data Breach Dropped 10 Percent Globally in 2017 Study

Cost in U.S. Continued to Rise as Europe Declined; Regulatory Differences May Dramatically Impact Breach Costs

CAMBRIDGE, MA – June 20, 2017 – IBM Security today announced the results of a global study exploring the implications and effects of data breaches on today’s businesses. Sponsored by IBM Security and conducted by Ponemon Institute, the study found that the average cost of a data breach is $3.62 million globally[1], a 10 percent decline from 2016 results. This is the first time since the global study was created that there has been an overall decrease in the cost. According to the study, these data breaches cost companies $141 per lost or stolen record on average.

Analysing the 11 countries and two regions surveyed in the report, IBM Security identified a close correlation between the response to regulatory requirements in Europe and the overall cost of a data breach. European countries saw 26 percent decrease in the total cost of a data breach over last year's study. Businesses in Europe operate in a more centralised regulatory environment, while businesses in the United States (U.S.) have unique requirements, with 48 of 50 states having their own data breach laws. Responding to a multitude of regulatory requirements and reporting to potentially millions of consumers can be an extremely costly and resource intensive task.

According to the 2017 Cost of Data Breach Study: Global Overview, "compliance failures" and "rushing to notify" were among the top five reasons the cost of a breach rose in the U.S. A comparison of these factors suggests that regulatory activities in the U.S. could cost businesses more per record when compared to Europe. For example, compliance failures cost U.S. businesses 48 percent more than European companies, while rushing to notify cost U.S. businesses 50 percent more than European companies. Additionally, U.S. companies reported paying over $690,000 on average for notification costs related to a breach - which is more than double the amount of any other country surveyed in the report.

"New regulatory requirements like GDPR in Europe pose a challenge and an opportunity for businesses seeking to better manage their response to data breaches," said Wendi Whitmore, Global Lead, IBM X-Force Incident Response & Intelligence Services (IRIS). "Quickly identifying what has happened, what the attacker has access to, and how to contain and remove their access is more important than ever. With that in mind, having a comprehensive incident response plan in place is critical, so when an organisation experiences an incident, they can respond quickly and effectively."

The Cost of a Data Breach Not Down Everywhere

In the 2017 global study, the overall cost of a data breach decreased to $3.62 million – down 10 percent from $4 million last year. However, many regions experienced an increased cost of a data breach – for example, the cost of a data breach in the U.S. was $7.35 million, a five percent increase compared to last year. However, the U.S. wasn't the only country to experience increased costs in 2017.

- **Non-European Countries Experienced Increased Costs:** Organisations in the Middle East, Japan, South Africa, and India all experienced increased costs in 2017 compared to the four-year average costs.
- **European Countries Experienced Most Significant Decrease in Costs:** Germany, France, Italy and the U.K. experienced significant decreases compared to the four-year average costs. Australia, Canada and Brasil also experienced decreased costs compared to the four-year average cost of a data breach.

When compared to other regions, U.S. organisations experienced the most expensive data breaches in the 2017 report.

- In the Middle East, organisations saw the second highest average cost of a data breach at $4.94 million – more than 10 percent increase over the previous year
- Canada was the third most expensive country for data breaches, costing organisations an average of $4.31 million.
- In Brasil data breaches were the least expensive overall, costing companies only $1.52 million.

Time Is Money: Containing Data Breaches

For the third year in a row, the study found that having an Incident Response (IR) team in place significantly reduced the cost of a data breach, saving more than $19 per lost or stolen record. The speed at which a breach can be identified and contained is in large part due to the use of an IR team and having a formal Incident Response plan. IR teams can assist organisations to navigate the complicated aspects of containing a data breach to mitigate further losses.

According to the study, how quickly an organisation can contain data breach incidents have a direct impact on financial consequences. The cost of a data breach was nearly $1 million lower on average for organisations that were able to contain a data breach in less than thirty days compared to those that took longer than 30 days. Speed of response will be increasingly critical as GDPR is implemented in May 2018, which will require organisations doing business in Europe to report data breaches within 72 hours or risk facing fines of up to four percent of their global annual turnover.

With such significant cost savings in mind, the study revealed there's room for improvement with organisations when it comes to the time to identify and respond to a breach. On average, organisations took more than six months to identify a breach, and more than 66 additional days to contain a breach once discovered.

Additional Key Findings from 2017 Cost of a Data Breach Report

- **By Industry, Healthcare Breaches Most Costly:** For the seventh year in a row, healthcare has topped the list as the most expensive industry for data breaches. Healthcare data breaches cost organisations $380 per record, more than 2.5 times the global average across industries ($141 per record.)
- **Top Factors Increasing Cost of a Breach:** The involvement of third-parties in a data breach was the top contributing factor that led to an increase in the cost of a data breach, increasing the cost $17 per record. Organisations need to evaluate the security posture of their third-party providers – from payroll to cloud providers to CRM – to ensure the security of employee and customer data.
- **Top Factors Reducing Cost of a Breach:** Incident response, encryption and education were the factors shown to have the most impact on reducing the cost of a data breach. Having an incident response team in place resulted in $19 reduction in cost per lost or stolen record, followed by extensive use of encryption ($16 reduction per record) and employee training ($12.50 reduction per record).
- **Positive Impact of Resiliency Orchestration:** Business continuity programs are significantly reducing the cost of a data breach. The overall average data breach cost per day is estimated at $5,064 in this year's study. Companies that have a manually operated Disaster Recovery process experienced an estimated average cost of $6,101 per day. In contrast, companies deploying an automated Disaster Recovery process that provides resiliency orchestration experienced a much lower average cost per day of $4,041. This represents a net difference of 39 percent (or a cost savings of $1,969 per day).

Uncovering the Cost of a Data Breach

The annual Cost of Data Breach study examines both direct and indirect costs to companies in dealing with a single data breach incident. Through in-depth interviews with more than 410 companies in 13 countries or regions, the study factors in costs associated with breach response activities, as well as reputational damage and the cost of lost business.

"Data breaches and the implications associated continue to be an unfortunate reality for today's businesses," said Dr. Larry Ponemon. "Year-over-year we see the tremendous cost burden that organisations face following a data breach. Details from the report illustrate factors that impact the cost of a data breach, and as part of an organisation's overall security strategy, they should consider these factors as they determine overall security strategy and ongoing investments in technology and services."

Download Full Reports & Register for the Webinar

To download the 2017 Cost of a Data Breach Study: Global Overview, visit https://www.ibm.com/security/data-breach/

Country-specific reports are also available for: the United States, United Kingdom, Germany, Australia, France, Brasil, Japan, Italy, India, the Arabian region (United Arab Emirates and Saudi Arabia), Canada, South Africa, and, for the first time, the Southeast Asian region (Singapore, Indonesia, the Philippines and Malaysia).

To explore and interact with findings from the 2017 report, please visit the IBM Security Data Breach Calculator, an interactive tool that allows you to manipulate report data and visualise the cost of a data breach across locations and industries, and understand how different factors affect breach costs.

To register to attend the IBM Security and Ponemon Institute webinar "Understanding Today's Security Breaches: Ponemon Institute's 2017 Cost of Data Breach Study" that will be held on June 26, 2017 at 11:00 AM EDT go to https://ibm.co/2ssR8qs.

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organisations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organisations, monitors 35 billion security events per day in more than 130 countries, and has been granted more than 3,000 security patents worldwide. For more information, please check www.ibm.com/security, follow @ibmsecurity on Twitter or visit the IBM Security Intelligence blog.

[1] Local currencies were converted to USD for the Global study.

Contact(s) information

Wilma Walsh

External Relations Manager A/NZ 0428955224wewalsh@au1.ibm.com