Announcements

IBM & Ponemon Institute: Cost of Data Breach in India rises by 12.3% in 2017

• Average cost of data breach rises from 97.3 million INR in 2016 to 110 million INR in 2017

Bengaluru - 20 Jun 2017: IBM Security (NYSE: IBM) has unveiled the results of a global study analyzing the financial impact of data breaches to a company's bottom line. Sponsored by IBM and conducted by the Ponemon Institute, the study found that the average cost of a data breach for the Indian companies surveyed has grown from 97.3 million INR in 2016 to 110.0 million INR in 2017 in India. Globally, the average cost of a data breach in 2017 is $3.62 million, a 10% decline from 2016. European countries saw a 26% decrease from 2016, whereas US registered a 5% increase comparatively.

IBM and Ponemon Institute examined Indian companies across 13 industry sectors who experienced the loss or theft of protected personal data and the notification of breach victims as per law. The per capita cost of data breach increased significantly from 3,704 INR (Indian rupees) in 2016 to 4,210 INR per compromised record. The number of breached records per incident for Indian organizations surveyed in this year's report ranged from 4,000 to 98,000 compromised records. The average number of breached records was 33,167 as per the study.

Malicious or criminal attacks were the cause of data breach for 41% of companies surveyed. About 33% experienced a data breach as a result of system glitches and 26% breaches involved employee or contractor negligence (i.e. human factor).

"The Cost of Data Breach study clearly outlines the rapidly changing threat scenario througha significant rise in both number and sophistication of breaches. With cloud services being the key for digital enterprise transformation, securing data on cloud is of top priority. Cloud Security and cognitive driven security services are going to be defining trends in the next years," said ***Kartik Shahani, Integrated Security Leader, India/South Asia at IBM*** *"Enterprises need to ensure that robust security practices are adopted, incident response plans are in place and regular security training given to all stakeholders of the company."*

Additional key findings and implications for organizations in India were:

- **For the first time, malicious or criminal attacks are the most common root cause of a data breach.**

Distribution of benchmark sample by root cause of data breach |Source: IBM & Ponemon Institute Cost of a Data Breach Study 2017

- **Malicious or criminal attacks are the costliest incidents:** Data breaches caused by malicious

or criminal attacks cost companies 5,100 INR per compromised record. System glitches and negligence (i.e. human error) cost 3,545 INR and 3,651 INR per record, respectively.

- **The more churn, the higher the cost of data breach** The highest cost as a result of customer churn was 125.1 million INR for companies whose churn rate was between 3 and 4 percent. The lowest was 91.6 million INR for companies whose churn rate was less than 1 percent.

- **Certain industries are more vulnerable to churn**: In this year's study, financial, technology and services industries experienced a relatively high abnormal churn. In contrast, public sector (government) and retail companies experienced a relatively low abnormal churn.

- **Detection and escalation costs increase**: 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 32.4 million INR in 2016 to 36.7 million INR in 2017.

- **The time to identify and contain data breaches impact costs**: In this year's study, it took companies an average of 170 days to detect that an incident occurred and an average of 72 days to contain it. If the mean time to identify (MTTI) was less than 100 days, the average cost to identify was 85.3 million INR. However, if the time to identify was greater than 100 days the cost rose significantly to 134.6 million INR. If the mean time to contain (MTTC) the breach was less than 30 days, the average cost was 96.3 million INR. If it took 30 days or longer, the cost rose significantly increased to 123.6 million INR.

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

Companies reported higher costs to respond to and remediate a data breach. To reduce the risks and consequences of a data breach, companies should consider investing in an incident response plan, the extensive use of encryption and threat intelligence sharing.

The most popular measures or steps taken after the data breach continue to be:

- Training and awareness programs (56%)
- additional manual procedures and controls (55%)
- the expanded use of encryption (40%)
- security intelligence systems (41%)

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 organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 20 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

For more information, please visit www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.