AJ Thompson

Chief Commercial Officer at Northdoor plc, the award-winning IT consultancy and services provider, that holds multiple accreditations from the largest of technology vendors including Microsoft and IBM, with over 30 years of experience serving blue-chip companies

Average cost of a data breach reaches $4.88m - a new record

IBM's annual 2024 Cost of a Data Breach report has revealed that the average cost of data breaches has hit a record high of $4.88 million. This is up by 10% from 2023 as breaches grow more disruptive and further expand demands on cyber teams.

The report is based on an in-depth analysis of real-world data breaches experienced by 604 organisations globally, across 17 industries, in 16 countries, with breaches ranging from 2,100 to 113,000 compromised records. It was conducted by the Ponemon Institute between March 2023 and February 2024 and is the 19th report to be published.

Increased costs driven by lost business

The average data breach cost has increased to a staggering $4.88 million from $4.45 million in 2023. This 10% spike is the highest increase since the pandemic. The report highlights that the rise in the cost of an average data breach was driven by lost business and post-breach customer and third-party response costs as the damage from data breaches increases. The report notes that the disruptive effects of data breaches not only drive up costs but also result in longer recovery times, with recovery taking more than 100 days in some cases. The cost of lost business and post breach activity has reached $2.8 million over the past six years.

Storing data across several environments

Alongside the 10% increase in average cost from a data breach, 70 % of breached organisations reported that the attack caused a significant or very significant disruption. One in three breaches involved shadow data, which shows that the rapid increase in data has made it harder to track and safeguard. Storing data across several environments accounted for 40% of breaches. This contrasts with data stored in just one environment, such as public cloud, on-prem or private cloud. These environments were breached far less often.

> "The average data breach cost has increased to a staggering $4.88 million from $4.45 million in 2023. This 10% spike is the highest increase since the pandemic. "

Personal customer data and intellectual property

The report found that nearly half of all breaches (46%) involved threat actors accessing customer Personal Identifiable Information (PII), such as emails, phone numbers, and home addresses. There was a 43% increase in the breach of Intellectual Property (IP) records, a considerable rise from 2023. The cost per record so far in 2024 is $173, compared to $156 in 2023.

Attacks taking advantage of employees and their company access also took a long time to fix. Phishing attacks lasted around 261 days on average, with social engineering attacks taking an average of 251 days to resolve. The report also cited malicious attacks by outside threat actors, or criminal insiders made up 55% of all breaches. However, as worrying as these figures are, it is important to remember that the remaining 23% are due to IT failure, and 22% are due to human error.

Understaffed security teams

IBM's report found that many organisations dealing with attacks struggled with staff shortages. Cybersecurity staffing shortages are up by 26% compared to 2023, with companies experiencing an additional $1.76 million in breach costs. This is starkly compared to companies with minor or no security staffing issues. This year's research found a strong link between the worsening skills shortage and higher data breach costs. Even with one in five organisations using Generative AI (GenAI) security tools to help them boost productivity and efficiency, the skills gap remains a problem.

According to analyst firm IDC, the situation is not expected to improve. IDC predicts that by 2026, more than 90% of organisations worldwide will feel the pain of the IT skills crisis. This amounts to some $5.5 trillion in losses caused by product delays, impaired competitiveness, and loss of business.

Gartner forecasts that the requirement of specialised training should be removed from 50% of entry-level cybersecurity roles within the next four years. This development will be welcome news to cyber managers, who have found recruiting increasingly challenging within the sector. Last year, The International Information System Security Certification Consortium (ISC2) found that the global gap had reached four million people, with 62 % of cybersecurity teams surveyed defining themselves as understaffed.

The growing use of GenAI should allow leaders to recruit based on aptitude rather than training or experience, dedicate more budget, and focus on filling critical cyber roles.

A notable and positive shift

The adoption of GenAI models and third-party applications across organisations, as well as the continuing use of Internet of Things (IoT) devices and Software as a Service (SaaS) applications, is expanding the attack surface, putting pressure on cybersecurity teams.

Over the last year, two out of three organisations have implemented artificial intelligence (AI) security solutions and automation tools, a notable and positive shift. Organisations that applied AI and automation to security prevention saw the most significant impact from their AI investments in this year's study, compared to three other security areas: detection, investigation and response. Those already using AI security tools were found to have incurred an average of $2.2 million less in breach costs than those not using AI. In fact, employee training and the use of AI and machine learning insights were the top factors mitigating average data breach costs.

It is clear that the implementation and management of AI and automated solutions are having a real impact on a business's ability to fight off a cyber-attack or keep costs and consequences as low as possible if a criminal did get through.

However, for those companies with small or even no internal IT teams identifying, implementing and managing such solutions is a daunting if not impossible task.

> "Organisations, their partners, and suppliers need to understand that just because defence systems were previously validated doesn't necessarily mean they are secure now."

Third-party IT consultants can help

Many are turning to third-party IT consultancies with the experience and expertise to advise on the most appropriate cyber defences and implement and manage them. This allows smaller IT in-house teams to focus on other critical business functions while having peace of mind that security is in the hands of a proactive and expert team.

As we have seen, the damage associated with a breach has never been higher. As IBM's 2024 Cost of a Data Breach report has shown, attacks are often difficult to detect and take a long time to fix, especially in large organisations with many partners and suppliers.

Organisations, their partners, and suppliers need to understand that just because defence systems were previously validated doesn't necessarily mean they are secure now. With many facing budget restraints and understaffing, rigorously assessing partners and suppliers may not be something that can be undertaken in-house.

With the average cost of a data breach reaching an eye-watering $4.88m and with internal teams unable to cope with the workload they already have, organisations need to turn to highly qualified, third-party IT consultants who can supplement internal teams. Third-party IT consultants can provide a 360-degree, 24/7 overview of an organisation, giving a comprehensive view of where vulnerabilities lie. This allows organisations to have urgent conversations with partners and suppliers to close the vulnerabilities before they are exploited by cybercriminals.

Data breaches are extremely lucrative and, therefore, will not go away any time soon. Getting ahead of any future attacks using AI, automation, and threat intelligence will be crucial for organisations. Effective prevention, detection, and response technologies implemented by third-party IT consultants will enable organisations to proactively defend against an attack.

Visit Northdoor to get the latest insights to take action against data breaches.