How to avoid data breaches while accelerating your digital transformation

By Chris Hockings | Chief Technology Officer, IBM Security, Asia Pacific

October 29, 2021

As the pandemic accelerated your need for digital transformation, you needed to act. And fast. And you were not alone.

But new findings from the recent IBM-Ponemon Institute *Cost of a Data Breach Report 2021* suggest that an organisation's pace of change may have an impact on the cost of data breaches. Respondents were asked to nominate the level of transformation occurring in their organisation due to the pandemic.

The report identified a 'sweet spot', where organisations with a 'moderate transformation' reported the lowest average cost of a data breach.

- The average cost of a data breach was US$5.01, the highest among organisations undergoing no transformation.
- The average cost per breach among organisations with 'very significant' transformations was only $750,000 less than those not undergoing any transformation.
- The cost was nearly 25 percent lower among companies undergoing a moderate transformation – representing a saving of US$1.23 million per breach on average

So, what can you do to embed security during every stage of your transformation?

Understand the risks of any cloud strategy and migration

The pace of change was only one factor. The report found breaches in businesses with highly complex IT environments – such as those largely dependent on legacy systems – cost 52 percent more than those in companies that have relatively uncomplicated designs.

Poor compliance was also associated with higher breach costs: it was 51 percent higher than in companies with effective compliance, according to the study.

As many businesses turn to the cloud to meet the many challenges of the pandemic, security should be an important consideration. Organisations aggressively shifting to cloud platforms reported an average cost per breach of US$5.12 million. That's US$1.66 million more than those with a low level of cloud migration during the reporting period.

The type of cloud platform and the stage of the migration are also important factors. Organisations in the early stages of their cloud modernisation journey took longer to detect and remediate a breach (329 days) than those with mature cloud practices (252 days).

Public cloud breaches cost US$4.80 million each on average, compared to US$4.55 million for breaches in private clouds. Hybrid cloud breaches cost even less, resulting in a 28 percent saving on average, compared to public cloud breaches.

It's clear that organisations embracing cloud platforms to support pandemic-era transformation should first fully understand the security implications of the shift – and consider how they can mitigate the risks. With security considered a key input to the design process, not only can a better risk posture be achieved, but the mechanisms needed to ensure continuous improvement will be in place.

Know the risks in your sector

The study also called out industries where rapid transformation, increased exposure or intrinsic complexity have left them struggling to transform as securely as other sectors.

Even as healthcare organisations fought on the pandemic's front lines, cybercriminal attacks cost them, on average, US$9.23 million. That's nearly a 30 percent increase in the May 2020–March 2021 period, compared to the previous year.

Costs surged even higher in other industries, with breaches in media organisations up by 92 percent. Other sectors with big increases included the public sector (up 79 percent), hospitality (76 percent), retail (63 percent) and consumer businesses (43 percent).

Conversely, sectors including energy, technology and industrial firms saw the average cost of data breaches fall over the same period.

Why would some industries see costs spike while others drove them down?

No doubt some organisations have better overall security than others. But another major factor could be that cybercriminals are targeting personally identifiable information (PII). We know that during the pandemic, as people had to become more self-sufficient, applying for new online services caused a spike of activity and led to user lethargy around password management.

Industries that rely on secure access – such as healthcare, the public sector and other citizen-facing industries – represent targets for cybercriminals who can exploit such weaknesses, gain access to personal information and sell it for considerable sums on the dark web.

Customer PII comprised 44 percent of compromised records, according to the report, and breaches involving customer PII were the most expensive per record on average.

Transform at the right speed with the right tools

While digital transformation is a critically important strategy for every organisation, the *Cost of a Data Breach Report 2021* confirms it can also create new problems if business data is not properly secured at every stage.

Fortunately, the report's findings suggest a number of emerging security strategies can reduce the cost of breaches. As explained in my previous article, the report identified security automation and protection of user credentials as vital measures for today's enterprise.

In addition, the report found the following tools and strategies can provide significant benefits:

- **Zero-trust security models** reduced the average cost of a data breach by US$1.76 million compared with companies that are still relying on conventional identity-management tools.
- **Incident response (IR) plans**, in which companies formed IR teams and tested their IR plans regularly, shaved US$2.46 million off the average cost of a data breach.
- **Endpoint protection** tools helped contain data breach costs, which increased by nearly 28 percent where remote working was a factor.
- **Encrypting data** to a high standard reduced data breach costs by 26 percent compared with companies with no or low-standard encryption.
- **Governance, risk management and compliance (GRC)** programs support risk management investments by quantifying the cost of a potential breach and the relative benefits of potential defences.
- **Security analytics** reduced average costs by 28 percent in companies that had established mature analytics processes.

Every company's transformation is different, but the *Cost of a Data Breach Report 2021* confirms that transformations are a time to be mindful. You don't want your transformation to introduce weak points that cybercriminals can exploit. The research shows that this is a real risk.

To minimise your exposure to data breaches, bake security into transformation processes from the beginning. Identify your potential weaknesses early – and address them before they leave you exposed.

What do you think? Have you been able to mitigate security breaches while transforming at a rapid pace? Do you need help? Connect with me here.

To learn more about how to control the cost of your next data breach, download the report here.

Article Categories

Digital Transformation | Security | Back to Stories