A Comparative Analysis of Breach Notification Policies in the Cloud Services Industry

By Ben Golopol and Otto Hanson

Cloud computing and storage is quickly becoming one of the most ubiquitous services used by businesses. A Flexera survey of 786 IT professionals revealed that 94% of respondents use cloud services already and 68% of respondents are spending at least $120k per year on these services.[1] Further, 38% of companies with more than 1,000 employees are spending more than $2.4m per year.[2] With so many resources being expended on cloud services, it is important for businesses to understand the terms of their agreements with cloud providers.

One of the biggest risks facing companies that host their data on the cloud is security breaches affecting their service providers. Such breaches can lead to the exposure of a company's data, including confidential information and personally identifiable information of both the company and its customers. As such, one of the most important provisions in a company's contract with its cloud provider is the breach notification policy, which lays out when and how the provider will notify the company that its data may have been exposed in a security breach. While some terms are more or less standardized across cloud providers, there are significant discrepancies when it comes to breach notification policies.

TermScout, a Denver-based startup that reviews click-through contracts, looked at the standard contracts for Amazon Web Services ("AWS"), Google Cloud Platform ("Google"), IBM Cloud ("IBM"), Microsoft Azure ("Microsoft"), and Oracle Cloud ("Oracle"). The table below describes their findings. When reviewing breach notification policies, it is useful to divide them into their constituent parts: the trigger (i.e. the event that initiates the provider's obligation), the timing (i.e. how soon after the trigger customers can expect to be notified) and the information the provider will include in the notification.

Data Breach Notification Policies by Cloud Providers			
	Trigger	**Timing**	**Information Provided**
AWS	N/A – AWS does not publish a breach notification policy	N/A	N/A
Microsoft	When Microsoft becomes aware of a breach affecting customer data	"Promptly and without undue delay"	Detailed information about the incident[3]
Google	When Google becomes aware of a breach affecting customer data	"Promptly and without undue delay"[4]	Description "to the extent possible" of details on incident, including Google's response[5]
IBM	When IBM becomes aware of breach "known or reasonably suspected" to affect customer data	"without undue delay"	Information about the breach and IBM's response, but only if "reasonably requested"[6]

Oracle	When Oracle confirms a breach affecting *any customer's* data that contains personal information	"without undue delay but at the latest within 24 hours"	Descriptions of the breach and reasonably anticipated consequences, Oracle's response, and "where possible," types of personal information affected[7]

Alone among these providers, AWS (the most widely used cloud services company in the world) does not provide any breach notification policy whatsoever in its contracts that we could find.[8] This means that AWS has no contractual obligation to alert its customers when their data may have been exposed to a security breach.

IBM, Google, Microsoft, and Oracle, in contrast to AWS, do at least provide a contractual policy. When it comes to triggers, Oracle stands out from the crowd because its obligations are triggered once Oracle confirms a breach affecting *any customer's* data that contains personal information, while Google, IBM, and Microsoft only have to notify a customer if the breach affected *that customer's* data.[9] Though Oracle's obligations are not triggered unless a breach affects personal information, the commitment is still significant because personal information is contained in most businesses' instances of the cloud.

On the topic of timing, each of the four providers with a policy promises to notify its customers "without undue delay" after the triggering event.[10] Though it may look good on paper, the vague nature of this qualification may leave providers some room to delay notification longer than some customers would prefer. When it comes to breaches, every minute that a company is unaware is a minute lost in response time. Oracle distinguishes itself in this category by placing an upper limit of 24 hours on its response time.[11]

In summary, there is substantial discrepancy among the cloud services industry leaders when it comes to breach notification policies. Considering the importance of response time when it comes to dealing with security breaches, it is important that businesses understand the differences in these policies and how they change the risk profile of using one provider versus another. In the authors' estimation, AWS's contracts are the least customer friendly when it comes to breach notification, while Oracle's are the best, with Google, IBM and Microsoft falling in the middle. For more detailed analysis on the cloud services contracts for the top five providers, visit termscout.io.

---

[1] Cloud Computing Trends: 2019 State of the Cloud Survey.
[2] Id.
[3] Security Incident Notification, Data Protection Terms, Microsoft Online Services Terms.
[4] Section 7.2.1, Google Data Processing and Security Terms.

[5] Section 7.2.2, Google Data Processing and Security Terms.
[6] Section 3(c), Data Security and Privacy Principles for IBM Cloud Services.
[7] Sections 8.2 and 11, Data Processing Agreement for Oracle Services.
[8] See Amazon Customer Agreement.
[9] Security Incident Notification, Data Protection Terms, Microsoft Online Services Terms; 7.2.1, Google Data Processing and Security Terms; Section 3(c), Data Security and Privacy Principles for IBM Cloud Services; Sections 8.2 and 11, Oracle Data Processing Agreement.
[10] Security Incident Notification, Data Protection Terms, Microsoft Online Services Terms; 7.2.1, Google Data Processing and Security Terms; Section 3(c), Data Security and Privacy Principles for IBM Cloud Services; Sections 8.2 and 11, Oracle Data Processing Agreement.
[11] Sections 8.2 and 11, Data Processing Agreement for Oracle Services.