netskope

WHITE PAPER

Evaluating Data Loss Impact

INTRODUCTION

To communicate the risk of data loss to an executive or board level audience, conversations and calculations need to move beyond the likelihood of an incident occurring. CISOs need to effectively assess the potential cost and reputational impact of an incident, in using data and terms in which the board is versant. However, while this ideology is not new, there are many good reasons why little progress has been made to move beyond the rhetoric and establish a usable methodology for evaluating Data Loss Impact.

Why calculate the impact of a data loss scenario?

- To ensure the risk is fully understood and prioritized at board level
- To ensure the necessary resources are available to mitigate the risk

Data Loss Impact is a hard thing to capture and a harder thing to action

Assessing the cost and reputational impact of a data loss incident can feel like more of an art than a science because the unknowns outnumber the knowns. It is incredibly hard to convincingly calculate the complex factors of a potential data loss incident because every organization will require its own formula based on its business model, market conditions, and the data it holds. Not all data is equal, and even within a single data set, value and associated risk can fluctuate dramatically over time.

Performing a risk assessment focused on loss factors always involves an amount of hypothetical future-gazing and conclusions can vary wildly depending on decisions to include or exclude certain factors.

Risk professionals often find themselves in a position where they can effectively communicate risk but do not communicate a clear proposal or the risks with the proposal. Furthermore when communicating the risk one must think about the ask and actions they are going to take to counter the risk. While we do not go into this in-depth, effective risk leaders will be able to understand and propose a wide range of proposals that allow the organization to address and manage the risk and not be stuck in a scenario where the risk “just has to be accepted.” An example of this would be proposing a full data governance strategy and program, proposing a scenario where users leverage new technology such as online collaboration vs. email/downloading of data, or proposing DLP solutions for a team vs. the whole company. The proposed options above would all address a data loss risk however all require different action and investment.

VALUING LOSS

Standards body, The Open Group, outlines six forms of loss to consider when measuring risk. Some are specifically associated with the lifecycle of an incident, while others are related to the business’ capacity to continue to trade normally. These six cost areas form a useful checklist and should be used to ensure that risk assessment calculations are comprehensive.

1) Loss of productivity

This category should capture any reduction in the organization’s ability to generate value from the core business proposition. In essence, it asks whether the data loss incident impacts day-to-do day operations and revenue in any way. This figure must use numbers that the board recognizes and agrees with, and ideally should map against the board’s expectations for company growth.

Productivity loss can occur in the short, medium, and long term, and it is advisable to map productivity losses against incident response timelines as outlined in policy and process documentation.

For cloud: When evalutating loss of productivity due to a cloud data incident, calculations may also include predetermining the business continuity and operational resilience of third-party service providers. CISOs should Identify whether access to data is interrupted if data loss occurs due to a cloud service failure. Service provider SLAs will usually specify the recovery time objective (RTO) if data needs to be recovered from a failure in their own, or their sub-processors, systems.

2) Response costs

This section of the assessment should detail all expenses which will be accrued in managing the incident. This will likely involve internal labor costs, as well as supplier fees. Policy and process documentation can be helpful in breaking down line items to include in this calculation, and ongoing operational expenses from DLP services should be included too.

For cloud: Audit information such as admin, user, and data access audit logs may be essential to efficiently manage incident response times and therefore costs. Not all cloud service providers offer this level of auditability, however investigating incidents and determining loss factors will require contextual traceability of this log data from a DLP engine.

3) Cost of replacement

While 'Cost of Response' covers assets that can be fixed or reconstructed, there will be others that are lost or damaged in a data loss incident that will need replacing. This value will vary widely depending on the nature and extent of the data loss, and whether it is just lost from the organization, or also lost to the organization (i.e. does the organization still have the data itself or does it need replacing). List prices can provide quotations on replacement infrastructure or hardware assets. Insurance costs (both third-party and warranty policies) with suppliers which would cover a data loss incident should be included here.

For cloud: Replacement cost listings should typically include the costs to replace a cloud service during an incident or post incident. As many cloud services are subscription based, the costs may vary, however the time and cost involved in shifting data to a new service should also be measured.

4) Fines and judgement fees

Calculations of data loss impact must include the legal or regulatory costs and fines that are incurred as a result of an incident. The formalization of data protection responsibilities is giving greater clarity to the potential fines that might be imposed after a data loss incident, with fines usually capped and identifiable in advance. The organization should keep up to date with international regulations and update this cost assessment regularly. While non-compliance fines are a secondary cost of a data protection infringement (the primary costs being the response and impact on business-as-usual) GDPR fines alone can be valued at 4% of annual global turnover or $20 million, whatever is higher.

For cloud: Shared liability and shared 'reasonable costs' need to be taken into account from a controller and processor perspective when fines and sanctions are issued and need to be appropriate to the procedural safeguards between the parties as per the agreement.

5) Loss of competitive advantage

Following a data loss incident, organizations can see a decline in the value of competitively differentiating assets. The value of individual data sets within large organizations is something that should be assessed and measured by individual data owners within each team (engineering, product, marketing, HR, etc). These data owners understand the lifecycle, value, and use of their specific data and should be working in collaboration with the information security team to ensure appropriate risk practices are followed.

Data value fluctuates based on a range of factors. Imagine that a company has invested $1 billion into R&D and product development. While this development is happening in secret, the confidential data relating to it will be of enormous value in terms of competitive advantage, but once patents are filed, the financial impact of disclosure drops significantly. The public launch of the product will further change the value of the data. The marketing campaign data will be high value to the organization until the moment it launches, when it will hold very little value at all. This is the same with mergers and acquisitions — much of the data in M&A activity is only sensitive while the deal is not yet public. If it leaks during the secretive phase, the entire deal may be jeopardized (along with the financial benefits the acquisition was to bring, a figure the board will be hugely aware of). Specific data held within individual files changes in value, but categorization of files can help manage this dynamism.

For cloud: In addition to the data itself, competitive advantage components may include algorithms tuned by the data for business intelligence and data analytics purposes. Data integrity is key to monitor for data poisoning attacks that may intentionally target machine learning through model skewing or feedback weaponization.

6) Reputational damage

The scale of reputational damage depends on the organizational business model, and the details of any incident. Losses associated with negative external perceptions of an organization as a result of an incident can be large, but often difficult to estimate. Marketing and communications teams should be able to provide some measurement of brand value, and help to assess the impact to brand and reputation of any data loss incident. Case study examples of the impact of incidents on other similar brands can be useful for illustrative purposes.

For cloud: Reputational damage may differ based on the category of data itself. As an example, customer data loss can lead to long-term reputational damage, especially if the organization has been clearly critiqued for poor organizational and technical controls in protecting the data. Historical instances have shown that the data-owning brand bears the brunt of the reputational damage, even when the fault lies with a third-party cloud provider.

Risk Exposure Area	Risk Exposure Impact Measurement	Risk Exposure Level (H/M/L)
Loss of Productivity	Hours lost, agreed-upon $ per hour, lost business opportunity	
Response Costs	Legal fees (external council), labor costs and supplier fees, stakeholder communication program	
Cost of Replacement	Service fees, labor costs, data acquisition costs	
Fines or Judgment Fees	Average $ per record, legal fees, labor cost	
Loss of Competitive Advantage	(Lost) market opportunity	
Reputational Damage	Customer confidence and revenue reduction, supply chain implications	

Probable Loss Magnitude (PLM) = Loss of productivity
+ Response costs
+ Cost of replacement
+ Fines and judgement fees
+ Loss of competitive advantage
+ Damage to reputation

VALUING DATA

No organization or industry body provides an easy to use, standardized table of data value for the CISO to attribute an agreed price tag to data assets, and therefore data loss costs are often not easily identifiable.

This paper has earlier touched on the difference between data being lost from an organization (which is a data protection issue) and data being lost to an organization (which is an added asset loss issue). When valuing data that is lost to an organization — i.e. data that is no longer an asset — professional services firm Genpact assigns three layers of value to aid in assessment.

- **Intrinsic value —** Where the sale of the data alone is a revenue opportunity, and its loss is comparable to the loss of boxed product.
- **Derivative value —** Where value is found by analyzing relationships between data sets, or acting on the data.
- **Algorithmic value —** Where the data unlocks value as part of a machine learning or otherwise automated business workflow.

A single data set may have multiple uses and its loss may impact multiple areas.

WHY NOT TO FOCUS ON THE MARKET VALUE OF DATA

It is tempting to look at the underground market retail value of data and consider this the cost of its loss to the organization. While this calculation can provide useful guidance as to the resources that malicious actors are prepared to expend on accessing the data (and potentially provide a threshold minimum that organizations should be prepared to expend on basic technical defences), it misses the point that an organization's data is worth more than the sum of its parts. To use a simple analogy — if someone steals your car and strips it down to sell off the parts for $5,000, that is a good day's work for the thief, but it is likely to cost you more than $25,000 to replace the car and cover your costs in the meantime. Is the knowledge that your car's parts might be worth $5,000 to someone else enough to justify your annual rent on a secure and CCTV-covered parking space? Probably not, but the fear of the $25,000+ risk cost might be.

The fluctuating cost of avoiding data loss

The principle of proportionality says that as the potential cost of data loss increases, so should the action undertaken to protect it.

The information security team, along with the appropriate data owners, should therefore be evaluating and categorizing data sets as closely as they study and protect potential attack surfaces. Neither data value nor risk are static, and as they fluctuate organizations need to identify ways to measure them dynamically.

CONCLUSION

Effectively calculating the impact of data loss on an organization is no easy task. It requires collaboration with business unit data owners and needs dynamic categorization and evaluation. Within the context of cloud infrastructure and storage, CISOs need to greatly improve visibility over data, its location, accessibility and use in order to accurately estimate data loss impact.

Without clear visibility, followed by a concerted effort to capture the impact of data loss in terms that resonate with executive teams and boards, data security threats cannot be effectively communicated. The Open Group's Risk Taxonomy technical standard paper is astute in stating, "a business manager tends to think of a "threat" as something which could result in a loss which the business cannot absorb without seriously damaging its trading position." To ensure that information security concerns appear on the business agenda as "threats" rather than "nuisances", we need to communicate them in the language of the business.