Ethical Technology Risk

How to Identify What Is Reasonable Data Protection for ODR

Chris Draper & Angie Raymond[*]

Abstract

This is a written representation of the presentation given on 29 October 2019, at 3:20 pm Eastern at the NCSC ODR2019 Summit held at the Colonial Williamsburg Lodge in Williamsburg, VA.

Keywords: ODR, security, data security, ethics, risk assessment.

There is no dearth of technology options that could be cobbled together into an online dispute resolution (ODR) solution. From commercial off-the-shelf (COTS) products to custom software, ODR solutions all require some mixture of integrated routines and manual processes that allow for a dispute to be acknowledged, all the relevant parties to be included, communication to occur between parties under varying levels of confidentiality, documentation of any agreement and archiving of any summary documentation. How these products, software and processes are assembled can have significant impacts on the appropriateness of any technology-enabled ODR solution. This presentation offers courts and other procurement professionals an assessment road map to ensure that any ODR solution proposed by a vendor provides reasonable protection of the disputing parties' data.

1 How to Assess Technology Risk

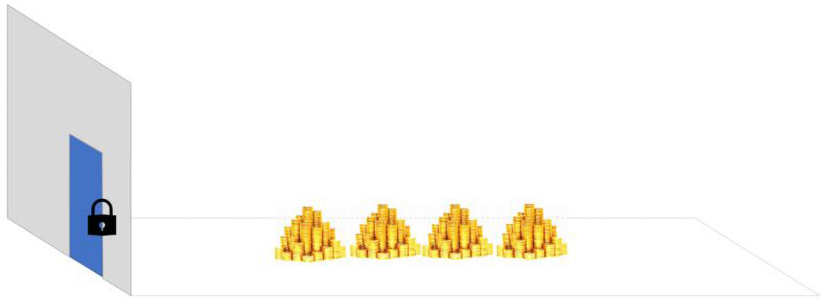
The risk associated with a particular outcome is the probability that the particular outcome will happen multiplied by the value of that outcome happening. When assessing the suitability of any system that is protecting data, it may be easiest to think of the data as a pile of gold sitting in the open.

Figure 1

* Managing Director, Meidh Technologies. Kelley School of Business, Indiana University.

The most common way to protect piles of gold is to put it behind a locked door.

Figure 2

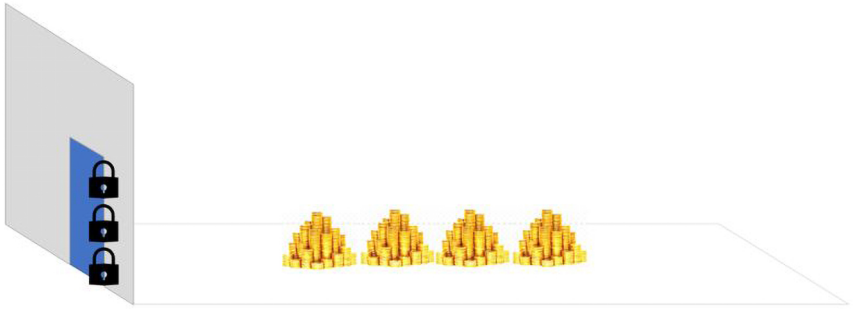


If the gold being protected is valuable enough, no matter what type of lock is used, there is a non-zero probability that any lock on any door can be broken open.

Figure 3

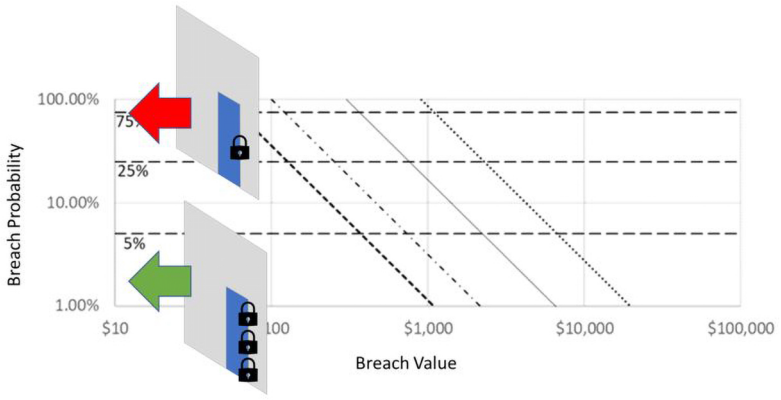
The most common way to reduce the risk from this type of breach is to put more locks on the door.

Figure 4



This approach to risk reduction focuses on reducing the probability of accessing the protected gold. In the case of data, this is achieved through techniques like multifactor authorization. When plotting data protection risk against its two axis of breach probability and breach cost, putting more locks on the door reduces the breach probability.

Figure 5

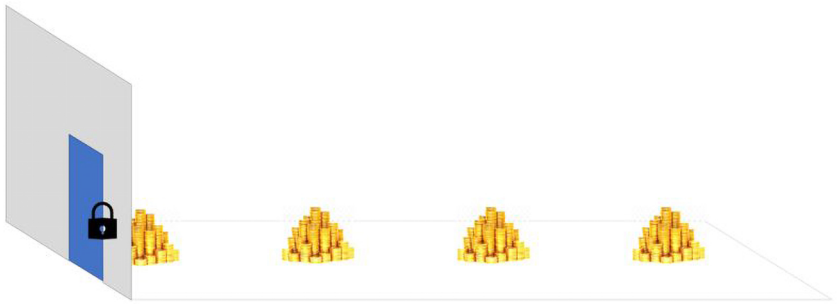


While most protection strategies focus on breach probability, there is only so much protection that can be employed before a system is unusable. For example, when multiple passwords and other authorization steps are required every time a user needs to log in, workarounds that negate such protection will always be found.

Risk can alternatively be lowered by reducing breach value. Looking back at the pile of gold behind a single door with one lock, breaking the lock provides access to all the gold being protected.

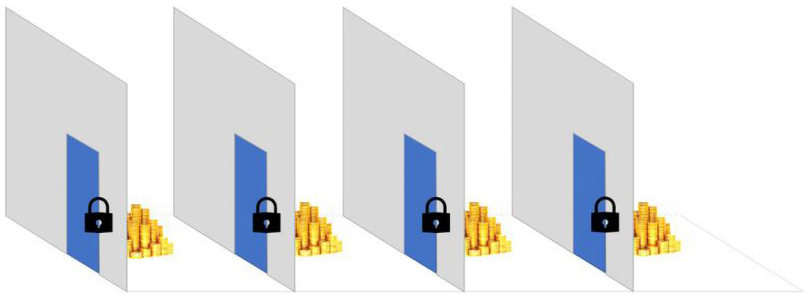
International Journal of Online Dispute Resolution 2019 (6) 2
doi: 10.5553/IJODR/235250022019006002004

Figure 6



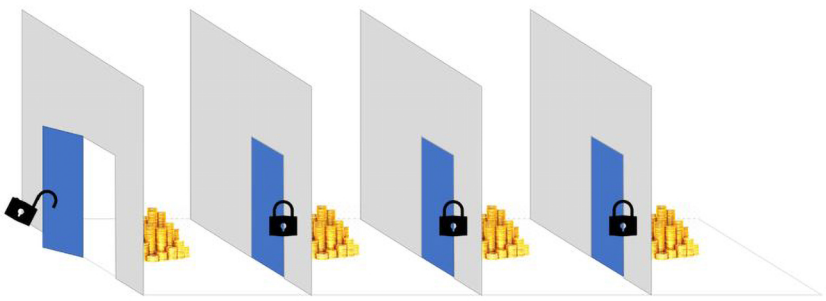
An alternative design strategy could allow for the gold to be separated into multiple compartments, each with its own protection.

Figure 7



By compartmentalizing the gold, breaking a single door will not provide access to the entire pile of gold.

Figure 8



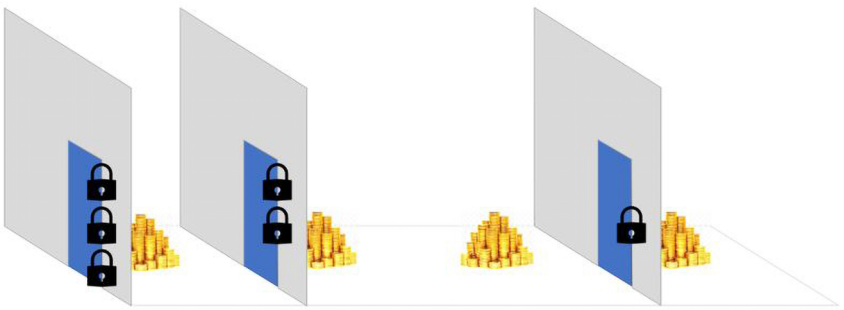
This approach to risk reduction results in lowering the value of a breach once it occurs. In the case of data, this would be achieved through data segmentation

strategies within database fragmenting or conditional permissioning practices. These strategies and practices ensure an individual who is within a system cannot move unimpeded throughout the entire system.

Figure 9

Most appropriately, system risk should be pursued through a mixture of breach probability reduction and corresponding consequence cost.

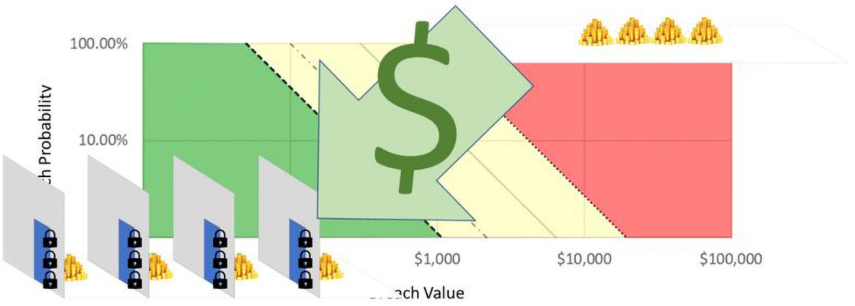
Figure 10



Finding an appropriate balance requires considering both probability and consequence reduction in the context of the economic cost required to make these reductions.

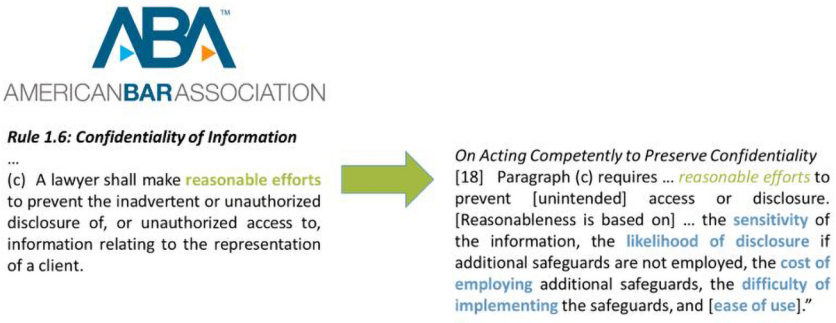
International Journal of Online Dispute Resolution 2019 (6) 2
doi: 10.5553/IJODR/235250022019006002004

Figure 11



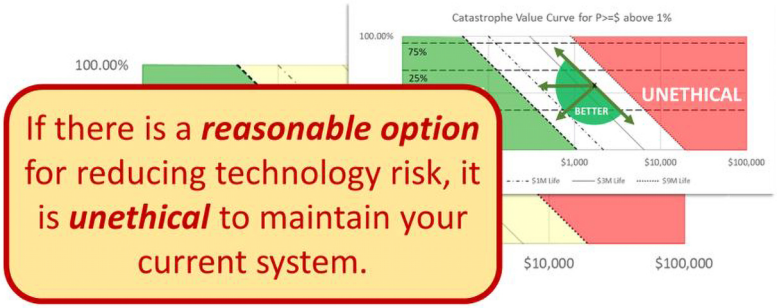
This need to balance technological risk and implementation cost is specifically called out in the definition of Reasonable Protection, as recently clarified by the ABA in the clarification to Rule 1.6.

Figure 12



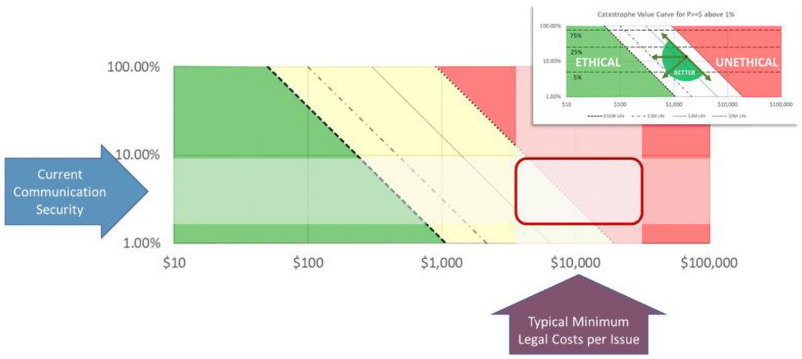
This relationship between security, usability and cost provides a basis for developing a risk-based relationship for defining 'ethical', wherein it is unethical to maintain a current system if a more reasonable, lower-risk option is economically available.

Figure 13



When looking at the practice currently used in the ODR space, given the current operational breach probabilities we are observing relative to the likely consequence cost associated with breaches, it is unethical for the traditional operator not to improve upon currently used systems.

Figure 14



However, as we look to improve upon our current risk levels, it is important to examine any alternatives from three primary perspectives: does our alternative ensure that any data is correct, does it ensure it remains unaltered, and does it protect the data in a manner that does not indirectly release any information of value.

When looking at these issues in the context of a 'smart contract', we should be looking at these risks from the perspective of any generalized, blockchain enabled system that draws in data from multiple, distributed sources so that it is immutably archived.

International Journal of Online Dispute Resolution 2019 (6) 2
doi: 10.5553/IJODR/235250022019006002004

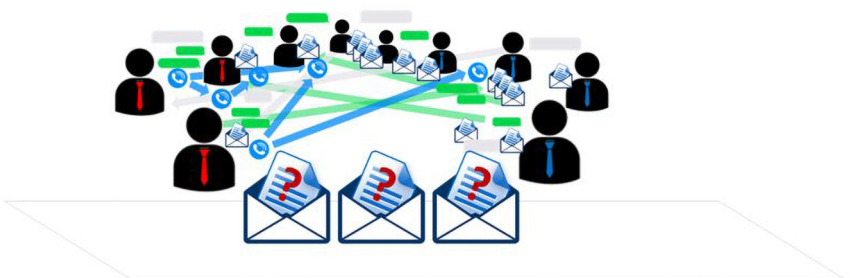
Figure 15

First, with respect to data correctness: *if we have a pile of gold, is it really gold?*

Figure 16

If we are using a system where communication error rates are significant, this risk of bad data being inserted into an immutable system does not fix the fact that the data is still bad. If anything, it makes the problem worse.

Figure 17



Second, with respect to persistence of data, *will it remain gold?*

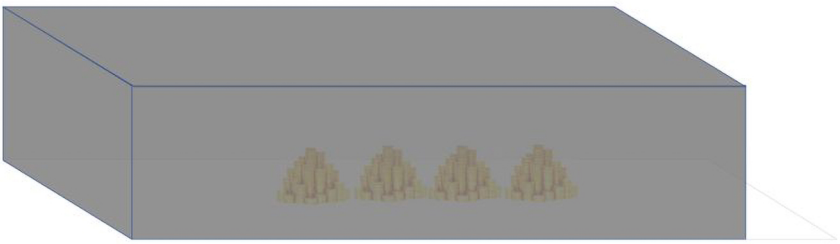
Figure 18

While there is much discussion about tools like blockchain that have the ability to ensure data will never be altered, it is important to consider both situations where the data should not be altered and others where the method of making data unalterable prevents it from being expunged in a manner as required by law. Immutability has the ability to be both good or bad, and its value must be assessed in the context of the technology's use.

Figure 19

Third, with respect to incidental releases, does the context reveal the gold?

Figure 20

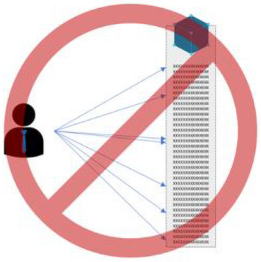


Many tools that are now intended to provide privacy – like encrypted emails – are at risk of being deployed in a manner wherein the value of the data being protected is still revealed owing to the fundamental nature of the vehicle being used. For example, an encrypted email from a divorce attorney sent to the client's partner will still reveal the nature of the data inside the email, thus causing an economic consequence that is fundamentally equivalent to the data being fully released. It is important that these contextual breaches are accounted for in any system being selected.

Figure 21

Accounting for these issues, especially in the blockchain space, is already seeing significant innovation when developed with a risk reduction focus. For example, Trokt has recently rolled out a 'neopublic' blockchain solution that addresses many of these issues by separating the context of data being written into a full node from the individuals writing it and separating the governance strategy for network use from the technological implementation of data validation and deconfliction.

Figure 22



Separates data context, so ***you cannot decipher user activity*** - *unlike a public blockchain*

Employs Static Proof of Stake, so ***Nodes are publicly governed*** - *unlike a private blockchain*

In the Trokt model, these types of innovations require careful consideration regarding governance strategy in order to ensure the technological innovations do not result in new failure mechanisms. In the Trokt network, these risk mitigation innovations in the underlying technology are supported with an Ostrom-based governance model that approaches network value as a limited community resource.

This strategy, like all others, will have strengths and weaknesses that must be assessed in a deliberate, systematic fashion. So long as the evaluation is focused on assessing how often an outcome can produce an approximate cost, with any economically accessible alternative selected when it can reduce the risk of a data breach, the improved system will be the ethical option for supporting ODR.