Trustwave®

For Improved Data Security, Burn, Baby, Burn

Consistent back burning, or deleting data when its value to the organization is limited, can starve hackers of a reason to attack you.

Consider this cybersecurity project: Its cost is extremely low, it's guaranteed to save you money, and it will significantly improve your risk profile.

This is Utopian. It's a unicorn. It's too good to be true. Right?

Well … no. We borrow a forestry term and call this back burning. What's the fuel for this fire? Data, of course.

Take away the fuel

As firefighters will quickly point out, the precise meaning of "back burning" is to intentionally set a smaller fire to burn against the one you're fighting, to consume the fuel in its path. We're using the term in a more colloquial sense; thinking of data deletion as a controlled burn. The idea is to eliminate a threat by robbing it of fuel.

Brushfires will occur, that's a simple fact. But their impact can be lessened through controlled burns. Data breaches, too, are inevitable; that's virtually a law of nature at this point in our evolution. But the impacts of such breaches can be reduced—sometimes dramatically—via back burning.

Data is what fuels a data breach. Lessen the amount of fuel and you lessen the likelihood, as well as the severity of a fire … er, breach.

The reality of regulation

Depending on your industry, you may be faced with a highly regulated environment, in which case concerns about deleting data you're obligated to keep are very real.

But keep in mind that even in such an environment, there is a cost associated with retaining information. And not just the cost of storage, but the cost associated with the average loss expectancy you incur by retaining that data. This cost is difficult to calculate precisely—but doing so might very well affect your decision.

Regulatory drivers aside, virtually all organizations are awash in what our firefighting friends would call "leaf litter" that can and should be burned:

- Old backups
- Databases for systems no longer in use
- Exports/extracts of data sets once used for analysis
- Random stuff the organization hangs on to … for no particularly good reason

About all of this sort of data, we can only say: Burn, baby, burn. We at Trustwave are hardly the only ones who grasp the relationship between data retention and infosec. As one clever expert said, "If you don't have it, it can't be stolen."

We have investigated data breaches involving data sets that should not have existed. One such case involved a client that was blackmailed based on actual data from an old database, to which attackers added wholly fabricated credit card numbers. The idea was to increase the perceived impact of the breach, in hopes of improving their likelihood of getting paid. It was a creative approach, to be sure, but only made possible by the company's failure to delete old data.

Costing it out

Here's the question at the heart of the matter:

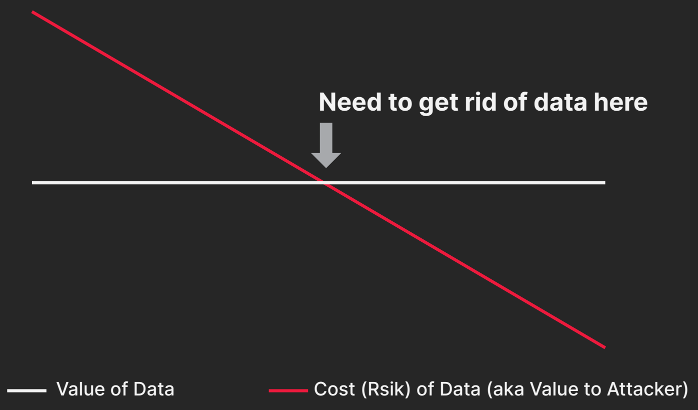
Is the cost (risk) of keeping data > the cost (risk) of deleting data?

The challenge here is that both sides of the calculation are difficult to turn into hard numbers. What's most important is to accept the premise that just as there is a cost associated with deleting data, there is also a cost associated with keeping it.

Here are a pair of thoughts that may at first seem surprising, given today's near-worshipful attitudes about data: Not all data is valuable. Moreover, the value of data to your business degrades over time, but the value of that same data to an attacker degrades less quickly.

Value vs Cost of Risk

Data loses value over time to your business, but the cost associated with the risk is static



For example, if a business has a record of a customer's last three places of residence, the value is quite low; the company's only real interest is in the current address. However, an attacker could use those old addresses to commit identity theft. So, the data-hoarding business has a downside risk without any upside. We would suggest back burning this information.

Reduce the reward

In the data security field, we typically focus on raising the cost attackers must pay for a successful breach. For example, it is said to be unrealistic to try to prevent a nation-state from compromising a company's network because the company cannot hope to compete with a nation-state on resources. By contrast, straightforward and inexpensive measures can make a successful attack too costly for most casual hackers.

But there is another, often overlooked, aspect to this equation: Why not reduce the reward to be gained from a successful attack? Back burning data does so at a low cost to the organization. We'll say it one more time: If you don't have it, it can't be stolen.

Getting started

Once you buy into the back burning concept, here are some recommendations to get a program up and running:

- Establish a Sensitive Data Environment (SDE). The SDE concept is similar to the Cardholder Data Environment concept in the context of the Payment Card Industry Data Security Standard; for our purposes, it refers to all systems processing or storing sensitive information.
- Build out a clear data deletion policy.
- Make data deletion somebody's actual job, to ensure accountability. That individual might, for example, run "data hunts," modelled on threat hunts, seeking sensitive data stored where it shouldn't be. If you can't create this position for budget reasons, you can at least deputize workers to perform the task, with appropriate incentives.
- Institute an amnesty period during which business units, departments, and individuals are rewarded for handing back rogue data.

Back burning seems almost too good to be true, but it's not—sometimes, the simplest solutions are the best ones.

To learn more about how to protect your data, check out the **Trustwave Proactive Database Security** webpage.

Trustwave®

www.trustwave.com