2022

# Data Vu: Why Breaches Involve the Same Stories Again and Again

Daniel J. Solove
*George Washington University Law School*, dsolove@law.gwu.edu



## Recommended Citation
Scientific American (July 2022)

SCIENTIFIC AMERICAN

# Data Vu:
## Why Breaches Involve the Same Stories Again and Again

*Data breaches involve the same old mistakes; we must break the cycle.*

By Daniel J. Solove and Woodrow Hartzog
Scientific American
July 26, 2022

In the classic comedy *Groundhog Day,* protagonist Phil, played by Bill Murray, asks "What would you do if you were stuck in one place and every day was exactly the same, and nothing that you did mattered?" In this movie, Phil is stuck reliving the same day over and over, where the events repeat in a continual loop, and nothing he does can stop them. Phil's predicament sounds a lot like our cruel cycle with data breaches.

Every year, organizations suffer more data spills and attacks, with personal information being exposed and abused at alarming rates. While Phil eventually figured out how to break the loop, we're still stuck: the same types of data breaches keep occurring with the same plot elements virtually unchanged.

Like Phil eventually managed to do, we must examine the recurring elements that allow data breaches to happen and try to learn from them. Common plotlines include human error, unnecessary data collection, consolidated storage and careless mistakes. Countless stories involve organizations that spent a ton of money on security and still ended up breached. Only when we learn from these recurring stories can we make headway in stopping the cycle.

The main plotline of so many data breach stories is human error. Over and over, people fall for phishing scams, fail to patch vulnerable software promptly, lose devices containing vital data, misconfigure servers or slip up in any number of other ways.

Hackers know that humans are the weak link. Many break-ins to company databases occur less by technological wizardry and more by con artistry. For instance, hackers can trick an organization's employees by sending an e-mail that looks like it's coming from one of their supervisors. Doing so is easy: anyone can readily learn the names of supervisors by looking them up on LinkedIn and can then spoof an e-mail address. Essentially, hackers hack humans more than they do machines.

Despite the fact that human error is an aspect of most data breaches, many organizations have failed to train employees about data security. As for the organizations that do, they often use long and boring training modules that people quickly forget. Not enough attention is paid to making training effective.

It's reasonable to expect that even with a well-trained workforce, some people will inevitably fall for hacker tricks. We must approach data security with realism that people can be gullible and careless, and human nature isn't going to change. That

means we need systems and rules in place that anticipate inevitable breaches and minimize their harm.

In many data breaches, an enormous amount of information is lost all at once. because hacked organizations were collecting more data than absolutely necessary, or keeping such information when they should have been deleting it.

Over time, organizations have been collecting and using data faster than they have been able to keep it secure—much like in the 19th-century industrial revolution when factories sprouted up before safety and pollution controls were introduced. Instead of hoarding as much information as possible, they should enact policies of data minimization to collect only data necessary for legitimate purposes and to avoid retaining unnecessary data.

To make matters worse, many organizations have stored the vast troves of information they amass in a single repository. When hackers break in, they can quickly access all the data all at once. As a result, breaches have grown bigger and bigger.

Although many organizations fear a diabolical hacker who can break into anything, what they should fear most are small, careless errors that are continually being made.

For instance, an entirely predictable mistake is a lost device. Lost or stolen laptops, phones and hard drives, loaded up with personal data, have played a big role in breaches. Companies should assume that at least some losses or thefts of portable devices will occur—and to prevent disaster, they should require that the data on them be encrypted. Far too often, there is no planning for inevitable careless mistakes other than hoping that they somehow won't happen.

Money alone is not enough to stop hackers. In fact, many of the organizations that have had big data breaches were also big spenders on data security. They had large security teams on staff. They had tons of resources. And yet, their defenses still were breached. The lesson here is that money must be spent on measures that actually work.

In the case of the Target breach in 2013, the company had spent a fortune on a large cybersecurity team and on sophisticated software to detect unusual activity. This software worked and sent out alerts—but security staff members were not paying enough attention, and reportedly they had turned off the software's automatic defenses. Having the best tools and many people isn't enough. A security team must also have a good playbook, and everyone must do their part.

Although at the surface, data breaches look like a bunch of isolated incidents, they are actually symptoms of deeper, interconnected problems involving the whole data ecosystem. Solving them will require companies to invest in security measures that can ward off breaches long before they happen—which may take new legislation.

With a few exceptions, current laws about data security do not look too far beyond the blast radius of the most recent breach—and that worsens the damage that these cyberattacks cause. Only so much marginal benefit can be had by charging increasing fines to breached entities. Instead, the law should target a broader set of risky actors, such as producers of insecure software and ad networks that facilitate the distribution of malware. Organizations that have breaches almost always could have done better, but there's only so much marginal benefit from beating them up. Laws could focus on holding other actors more accountable, so responsibility is more aptly distributed.

In addition to targeting a wider range of responsible entities, legislation could require data minimization. With reduced data, breaches become much less harmful. Limiting data access to those who need it and can prove their identity is also highly effective. Another underappreciated important protection is data mapping: knowing what data are being collected and maintained, the purposes for having the data, the whereabouts of the data and other key information.

Government organizations could act proactively to hold companies accountable for bad practices before a breach occurs,

rather than waiting for an attack. This strategy would strengthen data security more than the current approach of focusing almost entirely on breached organizations.

But the law keeps on serving up the same tired consequences for breached companies instead of trying to reform the larger data ecosystem. As with Phil, until lawmakers realize the errors of their ways, we will be fated to relive the same breaches over and over again.

---

*Originally published by Scientific American.*

*This is an opinion and analysis article, and the views expressed by the author or authors are not necessarily those of* Scientific American.

Daniel J. Solove is John Marshall Harlan Research Professor of Law at George Washington University Law School. He is the founder of TeachPrivacy, a company that provides computer-based privacy and data security training. Follow his work at his Web site www.danielsolove.com

Woodrow Hartzog is a professor of law at Boston University School of Law. Follow his work at his Web site www.woodrowhartzog.com

*This article is based on the authors' book Breached! Why Data Security Law Fails and How to Improve It* (Oxford University Press, 2022).