

*Regulators Should Rethink 'Reasonable
Data Security', Law360
(April 2019)*

Ryan Kriger



Regulators Should Rethink 'Reasonable Data Security'

By **Ryan Kriger** (April 8, 2019)

Your data is valuable — in the wrong hands it exposes you to identity theft, fraud and privacy violations. If a business collects your data, they are expected to prevent that data from being lost, stolen or wrongfully accessed. We call this legal requirement “reasonable data security.”

This might all seem obvious, but we must remind ourselves of first principles as we worry about data breaches, vendors that sell insecure software, and vendors that are entrusted with sensitive employee, customer or student data. It can be easy to get lost in the weeds, but the ultimate goal of the regulators is not to police data security — it is to protect consumers.



Ryan Kriger

So we must ask: Is this focus on reasonable data security protecting consumers? As a result of our enforcement efforts, is consumer data being kept more secure, except for a few bad actors? (There will always be bad actors.) If all the trainings and outreach we conduct, settlements we negotiate, and enforcement actions we bring, fail to protect people, then we must step back and reassess.

It is fair to say that data breaches remain ubiquitous and consumers do not believe that their data is being kept secure. A recent PricewaterhouseCoopers survey revealed that more than two-thirds of consumers believed that companies are vulnerable to hacks, and only a quarter believe that most companies handle their sensitive personal data responsibly.[1]

One can only speculate as to why we find ourselves in this situation after over a decade of enforcement in this area. Perhaps we just aren't enforcing enough given the scope of the problem. Perhaps businesses have measured the risk of both having a data breach and being investigated and have decided that the risks don't justify the costs of data security. Perhaps the market is set up to reward the fast deployment of insecure products, and punishes those who take a more secure approach. Perhaps the inconvenience that comes from real data security is more of a turnoff for consumers than the benefits that come from strong data security. Perhaps the bad guys are just that good and will always be one step ahead. Perhaps data security is just really hard and some businesses simply aren't good at it.

Despite this state of affairs, there is no question that the continuing diligence of the state attorneys general and the Federal Trade Commission is both worthwhile and necessary. Based on conversations with industry members, their counsel and their insurers, many businesses take data security more seriously than they would have were it not for our efforts. When a serious data breach happens, the citizenry expects there to be consequences, and it remains our duty as the states' chief law enforcement officers to hold these companies responsible. Though it might seem like the problem remains bad, it would be far worse were it not for our efforts.

And yet, things can certainly be better.

For businesses that wonder how they can obtain reasonable data security, there are many resources, but two good ones are the 2015 FTC report "Start With Security: A Guide for Business, Lessons Learned From FTC Cases,"[2] and the Massachusetts data security regulation 201 CMR 17, "standards for personal protection of residents of the

commonwealth."[3]

If you read these documents, you will see suggestions that should seem obvious to anyone working in data security. Encrypt sensitive data. Have a written data security policy and someone assigned to be accountable for it. Train your employees. Apply critical patches. Segment your network. These norms have been enforced for almost 15 years. A business that is not employing these steps is not simply lacking in reasonable data security — it is reckless.

But here's the rub: Compliance with these standards might help businesses avoid liability and keep consumers safer, but it will not guarantee safety from a data breach. That is because, as we know, data breaches will happen even to businesses with "reasonable data security."

This shows we need to rethink the way we have been evaluating data security. If you look at the two documents above, you will see that they are almost entirely about measures a business should take to prevent breaches. But completely preventing breaches is impossible. So, we must expand the definition of data security from an almost exclusive focus on prevention to a triangle that includes what happens before the data is collected, and what happens after the breach occurs.

In other words, we must focus on data minimization and breach detection.

Data minimization is a simple concept (though not entirely simple to implement): If you don't need the data, don't collect it because you can't lose data you don't have. The trend of the past decade has been for businesses to collect as much data as possible even if they aren't certain what they will do with it, and to hold onto it as long as possible in case they might need it. Businesses should do the opposite: Only collect data that they have an established business purpose for, and only hold onto data for as long as they need it or are required to hold it in order to comply with the law.

We should go even further than that, however. If businesses really want to avoid data breaches, we should consider technological advances that make obsolete the need to collect certain data in the first place. The fact that in 2019 we are still using a commonly exchanged 10-digit number to identify people, and an even more commonly exchanged 16-digit number to transfer money, is grossly reckless. Authentication technology that is not reliant on easily stolen static numbers exists. It is time to identify the most secure and reliable methods, bring down the costs and broadly adopt these technologies, and stop using Social Security numbers as a primary identifier.

Regulators can incentivize businesses to focus on data minimization by expanding our focus beyond how the data was lost to why the business was collecting the data in the first place, and whether it was holding on to the data longer than necessary. These questions are currently asked, and retention policies are considered as part of our investigations, but they rarely the primary focus of an enforcement action. This should change.

Where proper minimization can avoid many breaches entirely, detection is critically important because even in the event of a breach, early discovery can minimize harm to consumers, or if the detection takes place during the reconnaissance stage, essentially prevent the breach.

However, according to Verizon's 2018 "Data Breach Investigations Report,"[4] in 96% of cases breaches weren't discovered for months, and the breach is only discovered internally 40% of the time. Businesses may not be able to reliably prevent all breaches, but they can

definitely step up their game when it comes to detection.

Unfortunately, some businesses have poor data security because they simply don't want to know about breaches — if you don't detect it, you can't report it, and ignorance is bliss. Focusing on detection forces the ostriches to take their heads out of the sand. As an added benefit, detection will naturally lead to stronger prevention — a reasonable business that sees the magnitude of the efforts to penetrate their systems will harden its defenses.

While reasonable data security encompasses a broad spectrum of activities, the subset of reasonable breach detection practices is smaller and more manageable: For example, maintain your logs, monitor and aggregate your logs, implement intrusion detection systems, invest in services that scan the dark web, and only use cloud services that also maintain robust detection tools. Moreover, if organizations maintain programs that systemically inspect and analyze recent endpoint activity, obtain a complete activity timeline or forensic analysis, and gather details on incidents, breach detection and response will be much faster. There are software solutions and third parties that handle endpoint monitoring

Focusing on detection also simplifies the analysis for enforcers. The critical measurement is the window of compromise — the period of time from when a network intrusion begins to when it is discovered and contained. A very short window points toward a business that is on the ball — they were breached but they caught it quickly. A long window indicates a business that was willfully ignorant or asleep at the switch. Whether a business had reasonable data security is a frequent topic of legal debate, but the window of intrusion is a more objectively measurable and ascertainable metric. There will be situations where a business might argue that a large window is due to a sophisticated attack and an intruder that went to great lengths to hide itself, but these types of attacks are much less common than more typical breaches.

Regulators recognize that a business taking a year to discover a breach is bad, but it so common that it is hard to make that the sole focus of an enforcement action. We must change that norm as well. Much as regulatory efforts convinced businesses that prevention systems are necessary, we must emphasize that monthlong or yearlong windows of exposure are unacceptable and stress the need for detection systems.

Regulators should not abandon demands that businesses implement reasonable preventative measures, but instead enhance the definition of reasonable data security to a triangle that equally focuses on minimization, prevention and detection.

If regulators adopt this focus and the business community does the same, consumers will be safer, which is the ultimate goal.

Ryan G. Kriger is an assistant attorney general in the Vermont Office of the Attorney General.

The opinions expressed are those of the author and do not necessarily reflect the views of the Attorney General's Office or the state of Vermont, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] <https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/cybersecurity-protect-me.html>

[2] <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>

[3] <https://www.mass.gov/regulations/201-CMR-17-standards-for-the-protection-of-personal-information-of-residents-of-the>

You may also find the FTC cybersecurity for small businesses site useful. <https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity>

[4] <https://enterprise.verizon.com/resources/reports/dbir/>