IT Security: the rise of the data chemists

by

Timothy Grayson

830 words

The days of perimeter protection for online security and privacy are dwindling. Those tried-and-true approaches for safeguarding data and ensuring organizational and individual data security are destined to the quaintness of punch cards. Relying on them as the paradigm of security for extensive or elaborate IT implementations that have a future is not wise. There is a better way.

The concept of perimeter security is inspired by the notion that if you put all your eggs in one basket then you have but one basket to guard and protect. It is a castle, high on a hill with thick stone walls and drawbridges over impassable moats. The stuff inside is safe because the bad guys are kept at bay. Until it's not.

One problem with perimeter security is that it depends on meeting force with force. So attempts to breach firewalls and ports are met with clever shields and redundant blocks. That is not a bad thing; it's just a recursive cycle that probabilities suggest will always end in breaches. Moreover, it hardly matters how strong the perimeter is: once there is a crack, everything is in jeopardy. Since things have to move across the perimeter to function properly, the perimeter is porous by design, raising the odds of compromise.

To deal with the hole-y perimeter and make it reasonable for individuals to pass we take cues from the Old Testament. The Gileadites augmented their perimeter, keeping out the Ephraimites by

demanding everyone crossing the border say the word “Shibboleth.” To make an old story short, those that could not were obviously trespassers and were dealt with in a decidedly Old Testamentary way. The concept introduces the demand for secret password identification.

In prevailing IT security, a previously established password presented at the perimeter gets compared to the one held behind the perimeter walls. This system can be compromised on the *outside* by capturing the password or matchable token from the individual to whom it belongs. Alternatively, the store of passwords/comparables *inside* the perimeter is, in fact, a geometrically more valuable treasure.

This approach is ever-less effective. In fact, it is practically a law that *the value of perimeter protection is inversely proportional to participant sophistication*.

So, what is the viable alternative? In Introductory Financial Management many years ago, I was introduced to the concept of *diversification*. It refers to investing in assets of varying risk profiles so that the aggregate risk would be more readily predictable. There is a lot of calculus and probabilities math behind this, so it must be scientific. Those who avoid scientific language might be inclined to describe diversification as spreading the risk or *not* putting all your eggs in one basket.

Critically, the risk is inherent in the value of the asset itself. If data is the valuable asset and the risk is that its acquisition by unauthorized parties can result in privacy or confidentiality breach which could have significant financial impact, that sounds a bit more like securities. In which case, managing risk more like a financial wizard becomes sound policy.

This challenges a core assumption of today’s IT security, being that one can prevent breach from happening. In other words, we presume and measure *from zero*, trying to keep the needle there (like airline safety). After all, if there is a lot of valuable data in one spot AND breach will affect lots of data

and people, ANY breach is catastrophic and must be prevented. This base notion results in a course of action that takes us along the path that IT security has followed thus far.

What if that presumption were inverted? Instead, accept that there will always be (many) breaches. Then the goal cannot reasonably be to prevent them all, but rather to make them small, unprofitable, and essentially meaningless. In other words, diversify the risk away. This different starting point will result in a different approach. (That is the intent of encryption, but it should be quite evident that encryption alone is necessary but not sufficient in the cyber-security arms race.)

Take this idea further. What if there were no stores of meaningful aggregated data? It would not be worthwhile to penetrate the challenging security of an online service if there were nothing useful to acquire. Nobody would bother to break into a bank vault for one bar of gold. The crime doesn't pay. Such a circumstance would require CIOs and security specialists to become "data chemists." It is nothing less than alchemy—in reverse. Take gold and turn it into lead (or its elemental components). The real magic is in the owner being the only one able to reconstitute it into gold—when needed.

So, where does this leave us? Unfortunately, without specific answers; but with an idea for alternatives in the post-perimeter IT security world. The next wizards of security and privacy will succeed when they courageously change the metaphor and the starting point for their practice.

Start soon though: Our privacy and confidentiality depends on it.

XXX