In 2015, 60 percent of all attacks were carried out by insiders, either ones with malicious intent or those who served as inadvertent actors. In other words, they were instigated by people you’d be likely to trust. And they can result in substantial financial and reputational losses.

Nearly half of security incidents in 2015 were the result of unauthorized access. Unauthorized access has taken hold as the leading cause of incidents for our clients—as a 20-year-old vulnerability named Shellshock spurred a surge in unauthorized access attacks.

The healthcare industry was the one most frequently attacked, speeding straight past financial services and manufacturing. Healthcare moved into the top spot of the rankings as the most-attacked industry in 2015, replacing financial services, which dropped to third place. Five of the eight largest healthcare security breaches since the beginning of 2010 took place during the first six months of 2015. In fact, over 100 million healthcare records were compromised in 2015.

Cyber criminals didn’t stop for a break. While the average client organization monitored by IBM Security Services experienced roughly 35% fewer security events in 2015 than in 2014, our average client company was found to have experienced 64% more security incidents in 2015 than were discovered in 2014. The significant drop in the number of both events and attacks reflects specific and continually optimized policy tuning on the part of IBM security analysts, which allowed for far greater efficiency on all levels, cancelling out “noise” and making it possible for analysts to shift their attention to those events and attacks meriting further analysis.

There’s no place to hide. These findings reflect a change in the methodology we use to determine which industries were the most frequently targeted. Previously, we based our determinations solely on the number of security incidents experienced by each industry. For 2015, however, we incorporated each industry’s attack counts as well. 3 Defined by our analysts as encompassing various types of attempts to break into a network, a server or a database, such as exploiting a vulnerability to inject command code into software, exploiting a backdoor, or bombarding a system with random passwords in hopes that one will work.