"BUT I ONLY WANTED TO STEAL THE HARDWARE"

How Greed, Generosity and the Defense of Civil Liberties Put Your Mobile Data at Risk

BEACHHEAD®

SUMMARY

Some human traits are security hazards -- and not always because they are faults. As a matter of fact, some traits directly and deliberately engineer situations in which data leaks are more likely. In the wake of these behaviors, it is not weak security but human motivations that endanger data because data security is often secondary to (or contradictory to) these motivations, and because these motivations can lead to carelessness or lack of attention. Worse, these situations primarily arise when the party responsible for the data has no personal stake in the situation as the data that they're handling is often not their own. While this white paper is not a treatise on psychology or human and social behavior, the three examples of motivations and behaviors in this paper aim to illuminate how human behavior must be acknowledged by and be a central concern for any data security plan.

GREED AND THEFT

Greed and theft are familiar concepts to the world of data security. Data breaches such as the one that recently hit Target, where personal data such as credit card numbers are stolen maliciously, make for unfortunately frequent news fodder. However, stealing data itself is not the only means by which data becomes endangered. Hardware theft is also a major security risk.

Stolen hardware is a major problem in most major cities -- smart phone theft or loss has affected over 40% of residents in Miami, New York, Los Angeles, Phoenix, and Sacramento. In San Francisco, mobile phone theft accounted for nearly half of all robberies last year. The modern smartphone does not just have a bevy of personal information such as a detailed calendar schedule and scores of phone numbers and names and potentially addresses; no, the rise of mobile banking and other finance-related apps such as Mint mean that phones now host an increasingly large amount of private financial data – data that can be at the fingertips of criminals in a matter of seconds.

However, the offenders who steal phones often don't care about the potential value of that data on the phone. They steal smartphones for their resale value and the value of their parts. If there happens to be sensitive information on the smartphone, it's not the thief's concern or responsibility. While greed and theft are the primary motivators, it is not greed for data that's risking data.

Even more, these risks can plague enterprises for larger scale breaches -- ones that, because of their very scale, cause greater headaches. Take the recent example of Coca-Cola and a hapless employee that "only" wanted take the hardware off Coca-Cola's hands (the hardware was slated for disposal and the employee was in charging of doing the disposing). But in spiriting away 55 laptops over a series of years while blatantly disregarding protocol, this employee exposed the private information -- including the social security numbers -- of tens of thousands of Coca-Cola employees, as well as others who were affiliated with Coca-Cola.

In all these situations, greed motivated an individual to steal hardware for their personal gain, without thought to the data that hardware still stored. The conscientious thief may take security precautions with the hardware and wipe the data while an opportunistic one may trade on the data's potential value. Either way these situations show that diligent data security must consider human greed.

MORAL RIGHTEOUSNESS

Strong morals are not usually considered to be a character failing, but they can be when data security is paramount. These past few years have been plagued with a succession of leaks of sensitive information with the U.S. government playing the protagonist. Recently, the actions of both Chelsea Manning and Edward Snowden seem to have dominated the news. Both individuals purportedly took the actions they did in the name of civil liberties and a moral high ground.

The ethics, legality, and impact of their action can be argued and challenged, but it does not change the fact that important and high-security data was exposed due to this moral righteousness. While Manning has allegedly already leaked all of the information she stole, Snowden has been slowly leaking information over the past few months. It is up for debate how much more information Snowden has not shared and could still reveal.

Even if both these individuals could be completely absolved of the criminality of their actions and we could all agree on their moral fortitude, it would still not change the fact that sensitive information has been exposed with a high potential that it has been sold to or accessed by foreign governments. The ability of a single actor to share this kind of information constitutes a major security risk, and the compulsion to exploit this security risk is only heightened when an individual believes that they have the wherewithal to make an individual moral judgment that has widespread impact.

It would be silly to condemn strong morals and values, but the security-minded should take these risky behaviors into account. Manning and Snowden display how information in the hands of the morally righteous can be risky, especially if -- like Manning -- they choose to share the information indiscriminately.

PHILANTHROPY AND GENEROSITY

Rounding out our trifecta of human behaviors is another virtue that may lead to folly in the world of data security. Philanthropic actions are to be admired, and altruism should be a virtue we all cultivate. However, sometimes the good of giving can blind people to how their gifts can be risky.

In particular, donating computer equipment can be an easy way to help a charity out, either by giving the organization more equipment to work with or allowing the charity to raise money by selling the equipment. However, people doing the donating should be extra vigilant about the

information stored on the donated equipment.

More than once, these donations have resulted in data security breaches. For instance, then attorney and now Texas State Representative Aaron Pena, Jr. donated a computer to charity from his law firm. The computer was later purchased from a pawnshop, and the new owner found sensitive data still saved on the computer even though Pena's spokesperson told news sources that the machine's hard drive had been wiped before donation. In another instance, the police department in Champaign, Illinois donated 50 computers. Of those, one of the computers was donated to Champaign Consortium, where they discovered that the computers still held personal information – including the names and social security numbers – of 139 police offices. Information Technologies Director Fred Halenar notes that the personal information was not compromised or widely shared, but it does not change the fact that the information was exposed and vulnerable.

Donating equipment is an admirable gesture, but it needs to be coupled with an awareness of how transferring hardware can be a potential data security risk. We can praise the philanthropic among us, but even generosity cannot prevent the negative impact of a data breach.

HUMAN BEHAVIOR

Data security isn't all just the best encryption and the strongest passwords. They are subject to the whims and caprices of human behavior. For the most part, users can't be relied on for security 100% of the time -- just as no human is faultless 100% of the time. Moreover, the motivations for these behaviors don't always fit your obvious, malicious, "steal the data" narratives. When data is spread across organizationally-owned and employee owned devices, failsafes and stopgaps should be built into an organization's data security management. Organizations need to build security systems that, even if they trust their employees, do not rely on that trust for primary data security needs. Humans are fallable and fall prey to their own desires and blindnesses. Our data security should acknowledge that.