Are You Smarter than the TSA? (Hint: No)

Daniel E. Geer Jr. | In-Q-Tel
Bob Blakley

Our security community loves to beat up the US Transportation Security Administration (TSA). We chide them for security theater, for incompetence, and most important, for wasting our money by responding as the enemy intended, stimulated by their asymmetric attack.

The US Bureau of Transportation Statistics (tinyurl.com/p4f6m) tells us that 631,939,829 passengers boarded domestic flights in the US in 2010. The TSA spent money on each one of these passenger-boarding incidents. Its budget is approximately US$8 billion annually, but let's take out a few bucks for VIPER, for all those machines the TSA bought and didn't use, and for other non-air-travel activities. Say for argument's sake that the air-security budget was $6.32 billion in 2010. That means the TSA spent $10 per passenger boarding in 2010, or $10 per "target" per year.

How much do you think al Qaeda is willing to spend to get ONE passenger on ONE plane with a bomb? It turns out we know the answer: the 9/11 Commission concluded that al Qaeda spent $500,000 on the 9/11 attacks (tinyurl.com/k659n); compared with today's TSA budget, that's $500,000 versus $(10 \times 19) = \$190$ for an attacker advantage of better than 2,500-to-1. We spend $6.32 billion, al Qaeda spends half a million, and they outspend us 2,500-to-1.

Are you feeling superior? Don't. Pot, meet kettle.

You're probably unhappy with us for saying this. Breathe. Put down those pitchforks and torches and count.

How many client devices might host a logon to your company's systems? Certainly all your employees' company-issued systems, probably all their mobile phones, and possibly all their home computers and personal tablets, too. And then there are your partners' systems. Worst of all (both from the viewpoint of your ability to control security and from the viewpoint of sheer size of the device population), there are your customers' systems. Add them all up and call the result T (short for "targets").

Now call your company's annual security budget (in dollars) B. Divide. If your B/T is less than $10, you aren't smarter than the TSA. We'll even bet you a glass of good Scotch that you aren't. Here's why we're willing to make the bet.

As a percentage of revenue, Alinean says (for large companies) the IT budget is 3.2 percent (tinyurl.com/83mjoyy); Gartner agrees, stating 3.5 percent (tinyurl.com/8yuzuym). As a percentage of IT budget, Gartner says the average security budget is 5 percent (tinyurl.com/cp8lc4s); PWC says it's 8 percent (tinyurl.com/ckn3psv). Healthcare is worse: HIMSS says 53 percent of healthcare shops spend less than 3 percent of their IT budgets on security (tinyurl.com/cajpk7h).

Let's go with Gartner (full disclosure: one of us worked there). The two numbers together give us a formula for estimating the security budgets of public companies: security is about 3.5 percent of 5 percent of revenues. Call it 0.15 percent of revenues to keep the calculations simple.

Let's benchmark some companies.

In its S1 filing (tinyurl.com/7rt5xjl), Facebook claims 845 million monthly active users. Its financials (tinyurl.com/7q2xj7h) give its *entire* cost of revenue, which includes operations, as $860 million. If you throw in the entire R&D budget, you get $1.248 billion. If 100 percent of this is spent on security, it's $1.48 per monthly active user account, or, if you assume every user accesses the site from a computer and a phone, $0.74 per target per year. If you take Gartner's 5 percent estimate, it's $0.04 per target per year.

Someone who wants to take over your Facebook account has to spend only $100 to achieve al Qaeda's 2,500-to-1 advantage over the TSA. How bad is that? Pretty bad, but not as bad as it gets.

Copublished by the IEEE Computer and Reliability Societies

Twitter's revenues for 2011 are estimated at $140 million, which would give a security budget of $210,000 (!!!). Twitter has a little over 500 million users, so (assuming two devices per user) it could be spending as little as 1/50 of 1 cent per target per year. This is probably low, but it's probably not three orders of magnitude low.

Maybe social media is a bad example; social media companies have vast populations and low margins. Let's pick a more mainstream industry: energy. Direct Energy had revenue of $4.4 billion in 2011; it claims to be the US's largest energy retailer, with 18 million accounts. Our 0.15 percent formula gives it a $6.6 million security budget and, at two devices per user (the company allows online payments and is moving to smart meters), it spends approximately $0.20 per target per year. That's five times better than our estimate for Facebook, but still 1/50 what the TSA spends.

Maybe energy isn't a good example, either. Who hacks energy companies? Let's go to the top of the food chain: banks. JPMC revenues in 2010 were $115 billion. Our formula gives JPMC a security budget of approximately $172.5 million. Let's be generous and assume that banks spend twice as much on security, on a percentage basis, as other companies—we'll call it $350 million.

How many targets does JPMC have? We don't know for sure, but we can put a lower-bound stake in the ground: JPMC's 2011 annual report says it has 17,334,000 active online users. Let's say each of them has two devices (phone and computer), which translates to roughly 35 million targets. JPMC could be spending $10 per target per year on security—as smart as the TSA but not smarter.

Amex made annual revenues of $30 billion in 2010. Per our estimating yardstick, adjusted for banking, that's $90 million in infosec spending. Amex says on its webpage that it has 97.4 million cards in force. If each cardholder is online and has two devices, that's $0.50 per target per year in infosec spending.

Citi's 2011 annual report claims that it has 22 million branded credit card holders in North America; its 2010 revenues were $86 billion. So 0.3 percent of $86 billion is $260 million for the security budget, and 22 million times two devices is 44 million targets. That yields $6 per target per year.

These are just estimates, based on Gartner numbers and public figures, which are rough estimates of target sizes and security budgets. But how far off can the estimates be? Can any company on the list be spending 10 times as much on security as our estimates indicate? We doubt it. One hundred times? Inconceivable. Even at 10 times our estimate, no company on the list spends more than $100 per target per year.

Do you think our enemies will hesitate to spend $1,000 to attack a target? Do you think they'll hesitate to spend $10,000? We don't. We aren't smarter than the TSA. We can't win this spending game.

So what's the path out of these woods? We don't know, but we do know this: whatever it is, it'll involve us spending money on a smaller number of things. An asymmetric enemy makes us spend a dollar on every single thing that might happen while he or she spends money on the one thing that will happen, and that's a mug's game. ■

Disclaimer

The views expressed in this article are those of the authors and may not represent the positions of their employers.

Daniel E. Geer Jr. is the chief information security officer for In-Q-Tel. He was formerly vice president and chief scientist at Verdasys, and is a past president of the Usenix Association. Contact him at dan@geer.org.

Bob Blakley was the General Chair of the 2003 IEEE Security and Privacy Symposium. Contact him at bob.blakley@gmail.com.

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.