Quantifying Reputation Loss From a Breach

Lori MacVittie, 2012-16-05

#infosec #security Putting a value on reputation is not as hard as you might think…

It's really easy to quantify some of the costs associated with a security breach. Number of customers impacted times the cost of a first class stamp plus the cost of a sheet of paper plus the cost of ink divided by … you get the picture. Some of the costs are easier than others to calculate. Some of them are not, and others appear downright impossible.

One of the "costs" often cited but rarely quantified is the cost to an organization's reputation. How does one calculate *that*?

Well, if folks sat down with the business people more often (the ones that live on the other side of the Meyer-Briggs Mountain) we'd find it's not really as difficult to calculate as one might think. While IT folks analyze flows and packet traces, business folks analyze market trends and impacts – such as those arising from poor customer service.

And if a breach of security isn't interpreted by the general populace as "poor customer service" then I'm not sure what is. While traditionally customer service is how one treats the customer, increasingly that's expanding to include how one treats the customer's ***data.*** And that means security.

This question "how much does it really cost" is one Jeremiah Grossman asks fairly directly in a recent blog, "Indirect Hard Losses":

As stated by InformationWeek regarding a Ponemon Institute study on the Cost of a Data Breach, "Customers, it seems, lose faith in organizations that can't keep data safe and take their business elsewhere." The next logical question is how much?

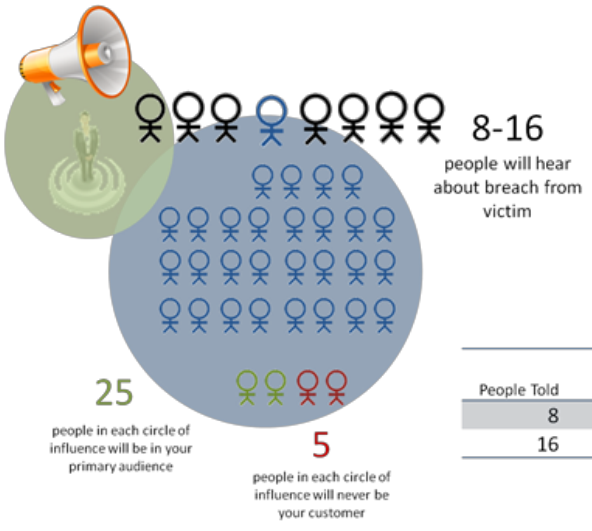
Jeremiah goes on to focus on revenue lost from web transactions after a breach and that's certainly part of the calculation, but what about those losses that might have been but now will never be? How can we measure not only the loss of revenue (meaning a decrease in first-order customers) but the potential loss of revenue? That's harder, but just as important as it more accurately represents the "reputation loss" often mentioned in passing but never assigned a concrete value (at least not publicly, some industries discretely share such data with trusted members of the same industry, but seeing these numbers in the wild? Good luck!)

HERE COMES the ALMOST SCIENCE

> 20% of the businesses that lost data lost customers as a direct result. The impacts were most severe for companies with more than 100 employees. Almost half of them lost sales.

Rubicon Survey

One of the first things we have to calculate is influence, as that directly impacts reputation. It is the ability of even a single customer to influence a given number of others (negatively or positively) that makes up reputation. It's word of mouth, what people say about you, after all.



People Told	Circles of Influence	Lost Future Customers
8	2000	40
16	4000	80

If we turn to studies that focus more on marketing and sales and businessy things, we can find a lot of this data. It's a well-studied area.

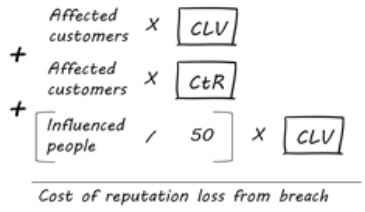
One study[1] indicates that the reach of a single dissatisfied customer will tell approximately 8-16 people. Each of those people has a circle of influence of about 250, with 25 of those being within an organization's primary target audience. Of all those told 2% (1 in 50) will defect or avoid an organization upon hearing of the victim's dissatisfaction.

So for every angry customer, the reputation impact is a loss of anywhere from 40-80 customers, existing and future. So much for thinking 100 records stolen in a breach is small potatoes, eh? Thousands of existing and potential customers loss is nothing to sneeze at.

Now, here's where it gets a little harder, because you're going to have to talk to the businessy folks to get some values to attach to those losses. See, there's two numbers you need yet: customer lifetime value (CLV) and the cost to replace a customer (which is higher than the cost of acquire a customer, but don't ask me why, I'm not a businessy folk).

Customer values are highly dependent upon industry. For example, based on 2010 FDIC data, the industry average annual customer value for a banking customer is $209[2]. Facebook's annual revenue per user (ARPU) is estimated at $2.00[3]. Estimates claim Google makes $9.85 annually off each Android user[4]. And Zynga's ARPU is estimated at $3.96 (based on a reported $0.33 monthly per user revenue)[5]. This is why you actually have to talk to the businessy guys, they know what these values are and you'll need them to plug in to the influence calculation to come up with a at-least-it's-closer-than-guessing value. You also need to ask what the average customer lifetime is, so you can calculate the loss from dissatisfied and defecting customers.

Then you just need to start plugging in the numbers. Remember, too, that it's a model; an estimate. It's not a perfect valuation system, but it should give you some kind of idea of what the reputational impact from a breach would be, which is more than most folks have today.



Even if you can't obtain the cost to replace value, try the model without it. Try a small breach, just for fun, say of 100 records. Let's use $4.00 as an annual customer value and a lifetime of ten years as an example.

Affected Customer Loss: 100 * ($4 *10) = $4000

Influenced Customer Loss: 100 * (40) = 4000 * 40 = $160,000

Total Reputation Cost: $164,000

Adding in the cost to replace can only make this larger and serves very little purpose except to show that even what many consider a relatively small breach (in terms of records lost) can be costly.

WHY is THIS VALUABLE?

The reason this is valuable is two-fold. First, it serves as the basis for a very logical and highly motivating business case for security solutions designed to prevent breaches. The problem with much of security is it's intangible and incalculable. It is harder to put monetary value to risk than it is to put monetary value on solutions. Thus, the ability to perform a cost-benefit analysis that is based in part on "reputation loss" is difficult for security professionals and IT in general. The business needs to be able to justify investments, and to do that they need hard-numbers that they can balance against.

It is the security professionals who so often are called upon to explain the "risk" of a breach and loss of data to the business. By providing them tangible data based on accepted business metrics and behavior offers them a more concrete view of the costs – in money – of a breach. That gives IT the leverage, the justification, for investing in solutions such as web application firewalls and vulnerability scanning services that are designed to detect and ultimately prevent such breaches from occurring.

It gives infosec some firm ground upon which stand and talk in terms the business understands: dollar signs.

[1] PUTTING A PRICE TAG ON A LOST CUSTOMER

[2] Free Checking and Debit Incentives Post-Durbin

[3] Facebook's Annual Revenue Per User

[4] Each Android User Will Make Google $9.85 per Year in 2012

[5] Zynga Doubled ARPU From Last Year Even as Facebook Platform Changes Slowed Growth

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com