

The Expert's Number for Security Risk Assessments

By **Donn Parker** – ISSA member, Silicon Valley, USA chapter

Author explains how to be an instant expert, establish a fact, and settle any argument by using a special “expert number.”

“We have become a worldwide society of numbers. We count and are counted. We measure and are measured... We are identified, codified, and described by numbers. Numbers place us in contexts of time, place, and circumstance... We can now reduce everything we do to a number language to be acted upon by machines.”

Printed on the wall of the IBM Museum, 590 Madison Avenue in New York City.

You can become an instant expert, establish a fact, and settle any argument by using a special number that I am going to tell you about. It is especially effective for establishing believable security risk assessment results. I have done considerable research to create this number and can assure you that it works exceedingly well. In fact, sometimes it works too well, spins out of control, and becomes perpetuated throughout the world in situations that you are not even aware of. As I lectured about security and computer crime around the world in such far off places as Jakarta and Johannesburg, when I asked my audiences a question that could be answered by a measurement, some smarty would shout out my number back to me.

Here is an example of how you might use this almost magic number. Suppose you want to gain c-management level approval for a new control that costs \$8580 in the first year of use. Suppose also that you estimate that management needs a risk justification of one order of magnitude savings over cost. Choose the risk assessment result to be \$85400 annual loss expectancy (ALE). Then work backwards and choose two numbers, one for frequency and the other for impact for incidents that might occur if the control were not in place that when multiplied together equals \$85400 (you may call it \$85.4K or \$85.4 thousand.) Your c-level management will accept the cost of the control because you can show them the cost estimate proof, but will they believe the risk estimate? Make sure that the frequency and impact look reasonable and support your choices with lots of wordy arguments. I chose \$85400 for you to use with intent because 85.4 is my univer-

sal expert's number and management will like that number more than others that you might try as I explain below.

You might be concerned that working backwards to derive a risk assessment that I describe in the security risk assessment example above is unethical. A chief information security officer at a large bank told me that this is the method that he uses quite successfully. When I complained that he was being unethical, he denied it and said that I didn't understand. He said that the numbers he uses represent a language as a means of communicating his expert opinion and nothing more, and management understands and doesn't question his numbers. He said that management just wants to believe numbers and satisfy auditors, boards, and regulators who are happy to see and believe numbers as well. Any reasonable numbers will suffice for security risk purposes (but don't use the universal expert's number too often.) Actually, this reverse risk assessment method is about as valid as starting with an incident, estimating frequency and impact, and calculating a risk, and it avoids getting a number that you can't use because it doesn't fit your purpose of the order of magnitude great than the control cost (in this case.) If you are very picky about your professional standing and ethics, you can work the method both forwards and backwards and adjust to suit your stakeholders.

You are exceedingly insightful of management if you use 85.4, the universal expert's number. Whenever you use it, it will make your management feel comfortable, nobody will challenge it, and all stakeholders will be confident in your expertise. Here is why you will be so successful. When expressed as thousands or hundreds of thousands of dollars, pounds, or Euros, 85 is most in that range, e.g., 85,000 between 10,000 to 100,000 or 850,000 between 100,000 to 1,000,000. If you used an even amount of money like 10,000 or 100,000 with a 1 and all of those zeros, it would be highly suspect as a number that you may have pulled out of a hat and not the real value of anything. So drop down to a comfortable 85. As a percentage, 85 is also most and a comfortable amount below a perfect 100%. It also represents a solid B as a grade in a class or on an

examination. It leaves comfortable distance between a real-life value and unbelievable perfection. The number 85 has an air of significance about it. It is close to 80 but a little more, and 80 is famous in Pareto's 80/20 rule that facilitates such generally known facts as 80% of the work is done by 20% of the people.

By itself 85 is a most comfortable number, but it is only two digits of precision and therefore looks like a rounded number making the victims, I mean your audience, wonder what that next digit of precision actually is in real life and whether any real work was done to obtain it. You really need three digits of precision for real world believability. Four digits are too difficult to remember, and nobody believes you can get four digits of precision as a real-world measurement of anything unless you are a physicist. 85 and a half (85.5) comes next in comfort, but this three-digit number is still a guess, and two 5s in a row detracts from variety. Moving a tenth off of .5 such as to .4 or .6 means that you must have done something significant to get the number but didn't expend an excessively exorbitant effort obtaining it. For example, in England the statistic of 2.2 children per adult female was felt to be in some respects absurd, and a Royal Commission suggested that the middle classes be paid money to increase the average to a rounder and more convenient number (*Punch* as quoted by M. J. Moroney.)

I actually invented 85.6, not 85.4 as the expert's universal number many years ago in the 1970s, but a friend of mine in Helsinki pointed out that 85.6 is the standard length of a credit card in millimeters and my number had suddenly become a real one; so I had to change it to 85.4, and I found that the new number worked just as well.

Back in the 1970s I first noticed that the public was going crazy in their need for numbers, and the number craze continues today. A problem or an issue was not sufficiently important enough, and a solution was not attainable unless experts could assign numerical measurement to it. Recently I counted 45 numbers on the front page of the newspaper. Wars are measured by the number of casualties, the disastrous terrorist attack on us by the date 9/11, the economy by the Dow Industrial average and number of lost jobs, anticipated elections by polls, and global warming by the rising number of inches of ocean water. Numbers have become mystical, and numerology has been on the rise ever since God identified 666 as the number of the Devil in the Book of Revelations in the Bible. After all, 85.4 percent of us are innumerate, and the rest of us don't know what this statistic means. Certain numbers are favored and shunned. China favors 8, and 4 and 14 are unlucky and are to be avoided. In the USA we favor 7 and avoid 13. For science fiction fans, 42 is the answer to the question of the meaning of life, the universe, and everything else.¹ Why not have a special number for special purposes such as expertise?

¹ Douglas Adams, *The Hitch-hiker's Guide to the Galaxies* (Pan Books, London and Sydney, 1979) was published based on a popular BBC Radio Series with the same name.

Computer crime became one of those big issues in the 1970s and the public was fascinated with this new form of crime along with Arthur C. Clarke, the science fiction writer who coined the aphorism that, "Any sufficiently advanced technology is indistinguishable from magic." Computer crime cried out for quantification just as risk-based security falsely does today in our field, and CSI along with the FBI try to satisfy the need for numbers. They are still producing hundreds of survey numbers of computer crimes every year with three or four digits of deceptive precision from statistically invalid, self-selected samples of security people, but the numbers are great and we see them frequently. When computer crime was new, information security experts were saying all sorts of crazy things about it to satisfy an enthusiastic public craving for enumeration. One was quoted saying that, "Only one in one hundred computer crimes is reported." Think about that for a moment. How would you know that there is only one if the others aren't reported?

I became the world's greatest expert on computer crime in the 1970s and 1980s when I was studying the problem, interviewing the perpetrators, and publicly reporting my findings based on my collection of several thousand cases (No, not 8540 thousand). Actually, it is only fair to say that I was also the world's worst expert on computer crime since I was the only one. Dan Rather on CBS 60 Minutes, Tom Brokaw on NBC Today, and Heraldo Rivera on ABC 20/20 who did special segments on computer crime and many other journalists almost ever day all asked me the same obvious question in interviews and over the telephone: "How much computer crime is there?" I got tired of saying that I had no idea (victims mostly try to keep it secret); so I needed a number and invented 85.6, now 85.4. I would answer their question with just, "85.4." And I could almost hear them salivate as they tapped it into their computers and then responded excitedly with, "85.4 what?" And I would respond by saying, "85.4 what ever you want it to be: 85.4% of all business crime, thousands of cases per year, percentage more than last year, percentage of more insider than outsider perpetrators. Just use my number wherever you need it in your article and it will satisfy your editor, make you an instant expert, establish a fact, and settle any argument." That seemed to satisfy some of them, and it caused the more perceptive ones to laugh, or become outraged when they caught on to my deception. But I would still read my standard answer of 85.4 printed in well-known newspapers and magazines, and you too can become an instant expert. Just use 85.4.

About the Author

Donn B. Parker, CISSP, is a retired senior information security consultant. He has specialized in information security and computer crime research for 35 of his 50 years in the computer field. He has written numerous books, papers, articles, and reports in his specialty based on interviews of more than 200 computer criminals and security reviews of more than 200 large corporations. He may be reached at Donnlorna@aol.com.

