2007-02
Measuring Security

Introduction:
Security metrics are among the most important and least well done things involved in managing security programs. What makes a good metric and how do we collect and present them? I'll give it a shot..

What makes a good security metric?
According to the American Heritage Dictionary, a metric is a standard of measurement, a function that ... describes the distances between pairs of points in a space. Security metrics that are useful describe something that can be measured about how far one security-related thing is from another. Let's explore just a bit more deeply:

- A useful metric should be repeatable in that two properly skilled independent parties measuring the same thing should come up with the same answer to within a defined margin of error.
- A useful metric should be used to do something with value exceeding the cost of measurement.
- A useful metric should be applicable over time to measure progress toward a defined goal and to measure differences between different things being measured.
- A useful metric should measure against some standard, and in security, a security standard.

Good security measurements have another property that I like to call sensibility. Someone who knows little about security but who s responsible for carrying out a security-related function should, when making the measurement or reading the measurement result, indicate that this makes sense to them.

Why would I want one?
There are a lot of things that can be measured, but measurement takes time, money, and thought that should not be wasted. The best reason to have security metrics today is to efficiently measure program progress. If the utility of the measurements cannot be understood by those being measured, they will not cooperate.

If you are trying to measure return on investment or some such thing, you are looking in the wrong place. The return on security investment is the survival of the enterprise every day. If you turn all security off, most enterprises will fail quickly. Low frequency, high impact incidents drive the largest losses and security losses are step functions. This makes baseline security metrics infeasible to measure over a continuous investment space. Each $1 in does not produce $2 out.

How do I collect them?
If you buy into the notion that the most effective security metrics today sensibly measure program progress against standards in a repeatable way, you are faced with how to do the measurements.

Program measurements of financial costs and progress against GANTT and PERT charts are widely available, but these sorts of mechanisms are not well designed to measure progress against security goals which do not involve finishing tasks but rather performing them in a repeatable and ongoing fashion. The data gathering from these sorts of mechanisms are also usually centralized, and while there are some designed for group project management, they are not oriented toward the sorts of things that security works toward.

Meaningful security program measurement involves things like these examples from ISO 27001 (ISMS):

- All information-related assets are identified and an inventory of important assets are accurately maintained.
- Adequate resources are provided to ensure that security procedures support the business requirements.

Each of these identifies a management judgment that has to be supported by documentation demonstrating how it is accomplished. There are about 250 such measurements for each individual responsible for content. While we could try to verify that every asset is reflected in an inventory system, the cost would be extreme and the utility limited. But ISO also demands that you measure your program. The solution lies in having people answer questions and verifying their answers by independent review. Human rewards and punishments are used to assure accuracy.

Conclusions:
Measuring security can be very effective at assuring that security programs make progress and that participants understand where they are going and how fast they are getting there:

1. Pick your metrics carefully to fulfill your real needs in a practical way.
2. Metrics have to measure realistic programmatic goals to be useful, used, and not abused.
3. Collection should not drive metrics selection, but metrics do have to be collected and analyzed.

Once you have a set of candidates, select the onces that will work best for measuring your program against a standard, create a system of measurement, and start.

Fraud of the month

Every month, we take an example from "*Frauds Spies and Lies and How to Defeat Them*" and describe a recent example. From page 47, section 2.5.5.6 we present the the Valentine's day heart breaker:

"Love Shack"

> *"Young women entice men into bed and then claim to be underage. They extort money from their lover and eventually may report them to their spouses anyway."*

Section 6.3.1.1.1 (page 183), "I'm old, overweight, and married" is my counter to all such attempts:

> *"I am overweight. I know it... If a gorgeous 22 year old girl comes up to me when I am on a trip, no matter how exhausted I am, I know that she is not there because I am her dream of a lover come true..."*

Love frauds are, unfortunately, all the more common at times of year like Valentine's day when people are looking for love and companionship and feeling lonely. And I would never be one to stand in the path of true love – or even temporary relief of the desire for companionship. But lots of people get seriously hurt, extorted, and taken advantage of in many ways by people who will trade their integrity and their body for whatever they want in life or think they need right now. So be careful out there. Enjoy the holiday and make good friends for life, and don't get paranoid. But stay aware that all that glitters is not gold and all that smiles is not love.

Chet's Corner

Love is in the air... or maybe that's just the pollen that's making me sneeze. At this time of year, we don't have any really good holidays to bolster our post-holiday season sales, so we invented a holiday surrounding love. After all, who can get away with not buying something for someone they love on Valentine's day? What a scam! And yet... I have in my hand a lovely bouquet and a box of candies. Love... it's hard to get around it. Secure your love by being extra nice every day!

"Always look on the bright side of life"!

Service Summary

Every month we feature one of our services and give an example of how it benefited one of our clients. This month it's our security measurement technology.

Some time ago I started to codify security knowledge into books and other literature. I found it useful to move it into programs that allow me to work more efficiently. This culminated in 2005 and 2006 with the creation of the CISO ToolKit – a collection of books and software that codifies much of what I know in terms that are readily usable and save a lot of typing.

A good example of its use was the process I used when a client asked for help integrating a recent acquisition. We decided to use a survey method to help gather information on the current security state of the business. *Surveyor* is used to do the data gathering and analysis with results reformatted for reporting. Reviews completed included:

1. Content inventory and risk levels
2. ISO-27001 compliance status
3. Management processes for security
4. Technical security elements present
5. Gap analysis against policy requirements

Initial surveys were done and then our independent review team came in to check results and help those taking surveys to provide better responses in the future. Results were then used to develop the next generation security architecture for the acquisition and ease transition to enterprise integration. Survey efforts took less than one hour per respondent (about ¼ of all workers were involved) the first time through and average about 30 minutes of effort per quarter for ongoing reviews that track progress over time.

Mollie gets the last word in

My boyfriend gave me chocolates,
which puts him in high regard,
My family sent me flowers,
which I planted in the yard,
My roommate made me cookies,
they came out sort of hard,
My heart goes out to you because,
you read this Valentine's day card.