2007-01
Closing the Gap

Introduction:

Gap analysis is one of the common techniques used in security management. But once you do or get a gap analysis, you still have a bigger problem. How do you close the gap?

What does a gap analysis look like?

This one may seem too obvious, but it's actually one of the key elements in closing the gap. The look and feel of the gap analysis relates directly to how you close the gaps and what gaps get closed.

- If the gap analysis consists of hundreds of technical elements all in a list, closing the gap is likely to consist largely of making minor and momentary repairs to identified flaws. It's a form of due diligence. We found a flaw now we fix it.
- If the gap analysis looks like a list of the elements of ISO 17799:2005 or an ISMS audit report from ISO 27001, you are likely to have a divergence with people arguing about issues and various attempts to 'kill the messenger'.
- If the gap analysis looks like a set of traffic lights in each of 10-20 areas, people will want to turn red lights into yellow lights and claim victory because yellow will be viewed as the baseline for success.
- If the baseline looks like a scatter chart, people will want not to be outliers and social pressure will cause most to seek the rest of the pack.
- The the baseline looks like a spreadsheet, people will try to analyze the numbers and optimize some summary information.

If your job is to close the gaps, you may want to use different looks and feels for different audiences.

People do what they can get done quickly

That is not to say that they get it done quickly. But rather, if you give a list of 10 things that they are supposed to get done, they will want to 'get as much done as they can' by getting the things that are easy to do done first, or put another way, by delaying doing the things that are hard.

If you are going to close big gaps, it is helpful to make it appear that all gaps are just as big. Pick the things you present in analysis and presentations by the granularity of effort to close the gap. If there are 40 minor technical flaws and 5 major management weaknesses, present all of the technical flaws in a single bundle so fixing all 40 are equivocated to fixing one management weakness.

Measure progress over time with pictures

I am probably the last person people would expect to advocate the use of dumbed-downed PowerPoints to explain how to close security gaps. And I don't advocate it. Use smarted up PowerPoints instead!

On my Web site, under the “Security Architecture” area, there is a clickable diagram of what enterprise information security architecture is all about. It was done in Open Office, not PowerPoint, but that's not the issue. People tell me that it's too complicated, and I tell them that it's nowhere near as complicated as the architectural drawing of their living room. Security is a complex field that crosses many boundaries. But that doesn't mean you can't measure and manage it reasonably well and present those measurements in a meaningful manner without dumbing them down.

- Start with a model of what things will look like when all the gaps are closed and keep things in terms of that model. Use mine if you don't have your own.
- Measure progress against the model. How useful is the business model of security utility? How comprehensive is oversight in coverage and participation? How well does risk management perform in the identified areas? How effectively does the CISO influence and measure all of the organizational perspectives and business processes? How embedded is security in the life cycles? How well does the control architecture meet security objectives?

All of these questions and many others can and must be put into terms of 'how much' and measured in repeatable and quantifiable ways if you are going to quantify the gaps and measure progress in closing them.

Conclusions:

Closing the gap can be greatly facilitated by remembering three key things:

1. Figure out who you are showing the analysis to and why you are showing it to them and show it in the form that will best inform.
2. Present gaps in roughly equivalent chunks of work so that closing 80% of the identified gaps doesn't result in doing 20% of the work that is needed.
3. Measure progress with sound metrics and present it with understandable pictures.

You can really only close the security gaps when you also close the communications gaps.

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 13, section 2.3.1.6 we present the start-of-year classic:

"Last year's money"

> *"Time is a funny thing in bookkeeping systems. Once the year is reconciled and closed out, it is largely ignored, but the database system that runs the computerized bookkeeping doesn't usually understand that, so... Take an account from the previous year that was not fully spent and use it to write a check to a vendor you have created for the purpose... The details may be a bit more complicated, but you get the idea..."*

Section 6.1.4.1.1 (page 173), "Currency Windows" is one counter to using last year's money:

> *"What is usually lacking is a... date window surrounding the date of entry... Anything that is entered into a computer that is not current should be questioned and independently reviewed. This is not just an indicator of fraud, but it is also a matter of business and process efficiency..."*

Time is of the essence in business. In many cases, the time required to do a thorough job of implementing technical protections surrounding financial systems is not taken to save on development costs. What you assume, fraudsters test and exploit. Take the time to do it right and you will avoid most time shifting frauds.

Chet's Corner

A new year and a new lease on life. The holidays are over and family and friends are back to their day-to-day lives, and as I look ahead to the year that awaits me, I think of how far I have come since a year ago and how far I will be going this year. January makes me shiver – with all the papers I will have to deliver... Time to get some Java going and get the new year kicked off. Have a super year and see if you can find me at the super bowl. I'll be next to the guy in the red jacket.

"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 the things we do for free.

Thirty years of information protection has produced a lot of results, and we like to share a lot of them with anyone who can use them. The all.net Web site is the place we use to share our results with the world. Yes – I know – everybody has a Web site. They are more or less free to own and worth what you pay to use them.

But our Web site is not like most Web sites. We like to deliver in-depth information with high utility for free. How do we make money at this? We don't. It's free. We hope it's helpful, and that's that. Sure, we would love to have you buy something from us, and we do sell things, but that's just because everyone who advises us on marketing says we have to. Here's what you can get without paying a penny:

- This newsletter every month.
- Several book and hundreds of papers on security-related subjects.
- Copies of recent presentations to various groups on up-to-date security subjects.
- Analytical database access with live analysis of select security-related issues.
- Security maps that cross-reference some of the most popular security standards and other works.
- A security architecture overview with pictures and drill-downs.
- A host of other informative articles and studies that you won't find anywhere else.

It's free, it's easy, and it's available for your viewing. All we ask is that when you use our ideas you cite our efforts and our site.

Mollie gets the last word in

As I wipe my eyes and try to get out of bed, I realize that the sun is not even up and I am writing an article for this rag on my laptop! What was I thinking? Oh... I remember. I was thinking that I have to get up, get dressed, and go out for my daily exercise. Some mornings I don't feel like it, but I know that it's the thing that keeps me alive and well. So off I go... Get your daily aerobics in and keep your heart smart!