2007-12
Security End-of-year

Introduction:

Business has end of year processes such as closing out the books, spending unspent budget, deciding what to do over the next year, and so forth. While this tends to go with the fiscal year that is not always aligned with the calendar year, whenever you decide to do it, security has its own annual cycles. At the end of those cycles, there is, or should be, and end-of-year process.

What should we do at the end of the year?

Tradition holds that the end of the year is the time when we look back at what we have done and look forward to what we will do. We reflect and plan, resolve to improve, and regenerate ourselves as to why we do what we do as well as how we do it. I am not known as someone who greatly respects tradition over reason, but I think that these traditions are reasonable, rational, end beneficial, so I try to follow them.

My security end of year has three phases. Yours will, no doubt, be quite different, but I thought I would offer mine as a straw man for your entertainment and consideration. Here are the three steps:

1. Do strategic review and conceptual planning.
2. Update policies, controls, and procedures.
3. Redo security decisions and other related things.

A step-by-step approach

Our strategic review and conceptual planning starts at the annual board meeting. As the overall strategy of the company is put forth, the needs for and approaches to the protection program emerge. The goal is to assure that the business functions as it should. Consequences of failures in information protection should be reasonably controlled from a business perspective to meet strategic business needs. From a tactical point, there are lots of things to do, but strategically, some things are important and some things are not. We focus on what's important to our business. This means that we identify specific things that we will need to do that we are not doing and other things that we are doing that we don't need to do. We plan to stop doing the things we don't need to do and to do the things we do need to do. This is usually done in October.

When I was younger I often complained and besmirched the checklist people, sometimes with good reason... But I have come to believe that a good checklist designed to allow for wide variation and thoughtful consideration is a good thing if well applied. Which is to say, I use a bunch of checklists to standardize and support my end of year process. Some of these are downloadable for free from my Web site (click on the Management Analytics logo and check them out), but many of them are not. We embrace standards to a point, so we do an ISO 27001 and 27002 review along with reviews of the Governance Guidebook and security Metrics approaches, usually in November or early December. This doesn't take very long because we already have it all done from last year. All we really have to do is go through it all from the beginning, identify the things we no longer have to do and the things we need to start doing, and codify it all. But that's the not as important as the fact that, in the process, we actually think through what we are doing and come up with improvements here and there. From that we make a list of all of the changes so we can prioritize them and measure progress against them over time.

The last thing in this sequence is to update our security decisions. Now this is the one where it's harder for us than for you. When we update our security decisions, we also update our “Security Decisions”. This is a software package we use to help our clients make their decisions, which means that is includes options for a wide range of enterprises and how they operate. So in updating the overall decisions, we also update our own decisions, making sure that we follow what we tell others to do and that we tell others to do what we actually embrace for our own operations. At the same time, we review the decisions for a few key clients or partners so that we get a reasonable coverage of the larger space and the larger issues.

How do I manage and measure this?

We have codified various aspects of these processes by using our Metrics software, and that allows us to go through and measure our progress in these activities and make sure that we actually do everything – or at least document having done it. That's just how it is. If we are audited, of course we will have to show that we actually do what we say we do, and we do, but that's not my job. OK - actually it is, but that's not what I'm discussing here.

We measure where we are and, over the period of implementation of changes, we go through and check off all of the things we have done and make comments regarding implementation issues, variances, and other things that come up. This produces reports that I personally review and check and, for certain ones, print and save in paper files.

Conclusions:

The security end-of-year process is a healthy one and one that I have come to embrace, not as a paper chase or another stupid mandate, but as an opportunity to align with the business. It allows me to stop doing things that ere no longer needed and start doing new things that are needed. Evolution is fun. At least I like it.

Copyright © Fred Cohen & Associates, 2008

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 14:

"Reorganization or one-time charges"

> "One of the ways I saw a large ($100 million) theft covered up was in a one-time bookkeeping charge at the end of the quarter. ... Of course this was just lying to the investors to keep them from running away..."

Do you know how to spell "Mortgage Refinancing"? Now you do. The sleazy financial industry players who have been buying and selling mortgages without doing any kind of due diligence have finally run into the wall, and unless there is massive inflation (look at the falling value of the US dollar for an indicator), the people who have these loans or the general public are going to take a financial hit in a big way. Probably both. These fraudulent schemes that trick people into buying things they cannot afford and then send them into homelessness and bankruptcy so that a few folks in the industry can make bit-time commissions by simply reselling the loans to others have paid off for the fraudsters and now the public is having to pay the price to help our fellow citizens.

Look for more of these huge write-downs in the next few quarters, and try to grin and bear it because there is nothing you can do about it except pull all of your money out of the financial industries, which will ultimately translate into your savings and investment holdings becoming worth less and less. The one thing we haven't seen is the fraudsters go to jail, and frankly, we are likely to be waiting for a long time...

Chet's Corner

The end is neigh! Repent!

Maybe the end is not really all that neigh, but a little repenting never hurt anyone, and it has helped a lot of folks over the years.

Sadly, this is the last article I will be writing in this series. Due to health and family issues, I will be spending more of my time focussing on life cycle issues and less of my time on the day-to-day issues of information security. I may be back, but for now, it is good luck for the coming year, and don't ever forget that you never know what tomorrow will bring.

"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 is our protection assessment and architecture design services.

> *In one recent urgent call for services, we were asked to offer alternatives to what was being done at that time to mitigate a serious problem that insiders were unable to make substantial progress on.*
>
> *They had a single-pronged strategy with no real architectural structures in place, and they were paying a high price every day. The one method they were using was not working, and it soon became very clear why it would never work given the nature of the problems they were facing. It was a mismatch.*
>
> *Our approach was to identify a set of different methods that applied to each of a set of different sub-problems in a divide and conquer strategy. By slicing the problem up we were able to create architectural structures that cut the size of the problem by 75% within three months and, over the lang run, would keep the problems from returning and reduce their impact if and when they appeared again.*

For some reason that we can never seem to divine, the last quarter of 2007 has been one of the biggest quarters we have ever had in this space. It seems to be the nature of this sort of work that it is feast or famine, and the last quarter of 2007 has been feast.

The common thread seems to be that architectural approaches and structures are emerging necessities to successful protection of enterprise value. And at the level of enterprise security architecture, there are very few strong players.

Mollie gets the last word in

I'm getting increasingly home sick, and during the holidays this becomes even more dramatic. So I'm happy to say that I am returning from South America!

The end of the year is a traditional time and I like my family traditions. We will be sitting in front of the fire place, going over the annual finances, planning for next year's home security improvements, and doing reviews of last years' lessons learned! I love it!

OK – so my family is a little bit weird. Isn't yours?

Copyright © Fred Cohen & Associates, 2008