2006-12
The Security Schedule

Introduction:

Many security practitioners work without a schedule, and one of the results is that they are always reacting to events instead of anticipating them. When we help develop security programs we find that one of the most valuable things we provide as output is the schedule.

What does the typical schedule look like?

The schedule for most security practitioners follows the same pattern as the enterprise schedule. It has periodic tasks that run year after year, and schedules associated with projects. Typical elements of schedules include:

- Training and awareness program acquisition, preparation, and execution.
- Internal and external audit and pre-audit preparation schedules.
- Personnel review schedules.
- Planning schedules for production of plans.
- Administrative coordination schedules.
- Budget schedules and timing for budget submissions and use.
- Group meetings including all of the groups coordinated by or involving the CISO.
- Holiday schedules.
- Coverage schedules associate with on-call duties and incident handling.
- Vacation schedules for workers.
- Legal compliance schedules.
- Procedural schedules for things like periodic backups and replacement cycles.
- Review schedules for things like periodic policy, standards, and procedures reviews.
- Business continuity and disaster recovery planning schedules.
- Risk assessment schedules associated with periodic risk reviews and updates.
- Project schedules associated with project phases.
- Zoning board meetings and similar enterprise-level architectural schedules.

It is fairly common for the preparation and meetings associated with this set of schedules to completely consume the time of the CISO, which is to say, the CISO is involved in all of these things. But those who work in information protection at all levels have responsibilities related to subsets of this list.

Controlling your schedule

Most people have problems knowing when and how to say “No.” at work. Controlling your schedule has everything to do with figuring out when and how to say “No.” Some of the practices I follow are included here to give you an idea of approaches that might work for you:

- I create meeting days and non-meeting days and try to push all meetings of similar type into time slots near each other on the meeting days. This grouping allows me to stay in the proper context for the meetings, prepare for them all together, and have a focused time period for work on a particular topic.
- The schedule is a tool for fending off unwanted or unnecessary meetings and activities as well as for creating favorable conditions for those meetings and activities. I don't ever publish my whole schedule using any sort of automated tool. This allows others to control the time and circumstances of my meetings and activities and to force me into things I don't want to do.
- I try to control the agenda and time frames for meetings. Generally, without an agenda or detailed subject and background for a meeting I won't attend. Such meetings often waste time and prevent me from preparing in advance. While some people may like surprises, security has enough surprises without meeting topics being part of them.
- I never schedule beyond 50% utilization in any given week. While a lot of pressure may be put on me to do so, I find that I need the other 50% of the time to do other things – like thinking about what I am doing, preparing for meetings, and responding to urgent situations.

My schedule is pretty busy, and most people in most enterprises today are so “efficient” that they have no time at all to figure out how to do things more efficiently or even how to prioritize the things that they do to best meet the needs of their enterprise. Learn how to say “No.” and you will do a better job both for you and for your enterprise.

Conclusions:

Security involves a lot of things and takes a lot of time and coordination to do well at the enterprise level. If you work in security, you need to get and formalize your annual, quarterly, monthly, weekly, and daily schedule in order to avoid the trap of “nothing to do” with a looming sense that you are missing something. There is plenty to do, and your schedule should show it – to you and others.

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 12, section 2.3.1.2 we present the ever popular end-of-year:

"Revenue smoothing"

> *"In revenue smoothing, the perpetrator actively reshapes revenue to meet predefined goals. For example, if you get a large bonus for making a sales quota each quarter but a smaller added bonus for additional sales over that threshold, then it pays to not book the closed sales after the goal is met and use them for the next quarter instead..."*

From section 6.1.4.1.3 (page 173), "Align rewards properly" is one counter to revenue smoothing:

> *"It is vital that rewards associated with behavior be aligned with the company's well being. People game the systems they work in to optimize their returns. If a company wants employees to do the right thing, they should build proper rewards and punishments for desired behaviors in proportion to their import to the company."*

When rewards escalate as value increases, it often reduces shifting revenues to the next period, but it encourages shifting from next quarter to this quarter. When combined with independent recognition of the source of the rewards, many types of shifting ahead are also eliminated.

Chet's Corner

My end-of-year schedule is hectic to say the least. Of course I have to finish the annual corporate and personal books, plan and execute holiday activities, close end-of-year sales, get payments and invoices in great shape, finish all otherwise unfinished work, and get annual reports out. But there is a secret end-of-year activity I do that keeps me sane. I get out of the office every day in December and take a few minutes to smell the roses in the busiest part of the day. Make time for yourself.

"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 long and strong experience:

Jan 1, 2007 will be the start of our 30th anniversary year of doing professional consulting in the computer security arena. This is a good point in time to look back on these 30 years to get a sense of the variety of work we have done and the range of things we can do for our clients. Here are some select projects that, while they weren't the most profitable of our efforts, we are most proud of:

- Designing secure protocols for early DoD voice and data networks (1970s).
- Microcoding special instructions into CPUs for special computing needs (1970s).
- Doing the first experiments on computer viruses and inventing most of the currently used defenses (1980s).
- Teaching short courses around the world in computer security topics (1980s).
- Identifying critical infrastructure security issues and defining "information assurance" as it is now used (early 1990s).
- Starting educational programs leading to the US CyberCorps (1990s).
- Creating bootable CD-ROM environments and components for secure computing, forensics, and intelligence (2000s).
- Research on cognitive limits of people and systems and its relationship to information protection and national security (2000s).

We have done many more profitable projects and an enormous variety of other work, but money isn't everything. In the end, its our contributions to the global community and the well being of the world that drives our efforts and defines us as a company.

Mollie gets the last word in

With a birthday between Christmas and New Years, I used to think that I was missing something because my party wasn't during school. But now I recognize that much of the World celebrates my birthday by taking a whole week off! Enjoy my birthday party and stay careful out there.