

The Security Consulting Sugar High

By Todd Kendall

It seems pertinent during this time of year, as I finish off the last batch of left over christmas cookies, some peppermint bark, and a large glass of eggnog, to talk about a phenomenon known as the sugar high. I'm talking about the high one gets after consuming large amounts of sugar, also called a "sugar rush." Sugar highs cause twitchiness, spasms, and hyper excitability. Sugar highs do not last very long and leave a person feeling drained afterwards.¹

As an IT Security Consultant I have had the opportunity to work with a variety of organizations over the years, often on multiple occasions and on multiple projects that stem from Security Policy Development, Gap Analysis, Penetration Testing, and in some cases Incident Response and Forensics. When you work with organizations in this capacity it is difficult not to develop personal relationships over time, and, as any good consultant will tell you, you want to gain a "trusted" relationship not only from an ethical point of view but also from a capitalist point of view. Let's face it, more trust, means more business.

Like any relationship, you may find yourself in a position at some point where you simply have to tell the other party that they simply aren't listening. Despite all of the times you have had the same conversation, and they swear up and down to take your advice.

Discuss in Forums {mos_smf_discuss:/root}

I've had a relationship with an organization that goes back to an original engagement I had with them in 2006. While some of the projects since that time have varied, the overall annual Statement of Work included an external/internal penetration test, an ISO Gap Analysis, and typically some type of social engineering exercise. In 2010, I highlighted the following section in my Executive Summary Presentation and asked the audience why they thought I was calling it out in red:

- Finalize the information security governance procedures
- Create a set of detailed formalized information security policies
- Prioritize and implement strategic initiatives as they relate to meeting staffing, budget, and compliance requirements
- Perform regular password audits
- Review and revise System Hardening program to include applications
- Conduct security assessments upon release of new application versions or major code revisions
- Implement Security Awareness program based on framework provided

At the risk of jeopardizing my relationship with the organization, and God forbid losing repeat business, I explained to the personnel in attendance that this slide had not changed in the last four years. Each year I had sat in the same briefing center and delivered equivalent findings from years past. Unfortunately, that particular year demonstrated that the lack of follow-up from previous years led to a major vulnerability stemming from past low risk findings. Over time, low risk findings or a combination of those findings have a way of becoming high risk issues, something I had been documenting in my reports the entire time.

Interestingly enough, each year's executive briefing was a very serious matter. Not only did management appear to grasp the situation and agree to support future security endeavors, but also the technical representatives who would have to perform the follow-up work were excited about the opportunity to fix the problems that had been discovered. These representatives thanked me and my colleagues for bringing these matters to the attention of management, so that the issues could be resolved, determined that their concerns had been addressed and that appropriate time and resources would be dedicated to mitigation in the near and long term. So, what happened? The Consulting Sugar High!

Why Does It Happen?

There can be a number of reasons an organization contracts consulting services. Whether for compliance, independent review, or as part of their system development life cycle, organizations are all seeking confirmation or advice. Those organizations that seek confirmation typically don't go through a consulting sugar high. These organizations have taken the time to answer most, if not all of the questions they wish to have confirmed. It comes as a general shock

should the report they receive point out any new findings disparate from their own efforts. These organizations may also be seeking advice, but even then that advice typically confirms one of the approaches they have discussed for handling any issues discovered moving forward. Alternatively, those organizations solely seeking advice are ones that approach security not from a cultural aspect, but from a checkmark mentality, i.e. we performed a security audit – check!

Organizations of the second nature find themselves asking numerous questions throughout the consulting service. When those questions are answered in a succinct and detailed manner it leads to additional interest and generally sparks excitement. How often do we find throughout the course of the day when questions are answered with a dismissive one sentence answer? IT Security Consultants are a different breed. They like what they do and are more than willing to go into excruciating detail about their opinion on security matters. They also like to show off their knowledge, which has likely resulted from hours of research. By the time the consulting service concludes, numerous conversations and a growing sense of excitement has grown throughout the organization as they await the final presentation or report. I'd like to say that all my presentations lead to even more excitement, but they can often become confrontational, lead to a sense of denial, and can unfortunately initiate finger pointing and blame. However, when presented with guidelines, roadmaps, and solutions, then the excitement from those earlier conversations spills over to management who now has a decisive plan for security moving forward in cooperation with their own organization's objectives. At this point, the consultant has finished their given task and departs. The organization is left with a high which I guess could be equated to twitchiness, spasms, and hyper excitability.

Regardless of whether or not a project plan is put together to embrace the consultant's advice, roadmap or solutions, within a few weeks the organization begins to come off their high. First, without the consultant there to continue to answer questions, the initial interest begins to fade; out of sight, out of mind. Second, a realization sets in as the personnel assigned to mitigate the issues discovered during the engagement find out their workload was just increased. Most organizations I know cannot afford to assign new or more resources to security issues as resources are always constrained. Third, even if management is supportive of the endeavours to increase security and reduce risk for the organization, their strategic plans and objectives have not changed. While mitigation efforts may have been prioritized at the conclusion of the engagement, those efforts will always fall below that of original management objectives. The only time I've seen this change is when the potential for substantial monetary consequences is at stake, i.e. regulatory compliance violations. The result is the end of the consulting sugar high, which did not last very long and leaves the organization feeling drained afterwards.

How Do You Avoid It?

I wish the answer to this phenomenon was as simple as the answer to avoiding sugar highs, i.e. don't be a glutton, all things in moderation, etc. But, then again, maybe it is? Until this past year when I took vacation, my busiest time of year has been the holidays. Why? Organizations wish to use up their budgets at the end of their fiscal year, which for many is also the end of the calendar year. As such I see an increase in projects during this time period. But, it isn't just an increase in projects because of an increase in the number of clients; it is an increase in projects per organization. As I mentioned above the Statement of Work included up to four projects. The presentation they received was a culmination of each of those projects into one executive presentation. The organization was simply inundated with information and thus mitigation efforts of their own accord.

So what is the easiest way to avoid the scenario above? Plan your consulting engagements throughout the year, give yourself time to focus on and address any issues discovered during those engagements, and plan on follow-up engagements to provide closure to your efforts. I have a colleague who always asks his customers, “How do you eat an elephant?” The answer is, “One bite at a time!”

Break your consulting engagements into bite-size manageable efforts. If you want to have four consulting engagements

completed by the end of the year, break those efforts into quarterly efforts. By breaking the engagements down you avoid a conclusive departure by the consultant. You know they will be coming back and the interest and excitement generated during those efforts is regenerated during the next visit. In addition, any questions during your mitigation efforts can be reviewed and readdressed in person. Issues identified during these efforts should decrease as the focus of the engagement is limited from one visit to the next. This should also remedy your resource constraints as mitigation efforts are a direct correlation of issues discovered. By taking this simple approach an organization will find that they have the ability to marry security efforts with management objectives and aren't scrambling at the end of the year... or grumbling through yet another "Consulting Sugar High."

Of course this is only one possible solution to the high fructose scenario. Being that The Ethical Hacker Network is not only an online magazine but also a community of professionals; my hope is that this article will spark debate. Am I full of it or do you see this as well? How have you addressed it? What other suggestions or war stories can you share with the rest of us? Join us in the dedicated forum thread for this article to continue the conversation.

Footnote 1: Definition courtesy of the Urban Dictionary

Todd Kendall is an experienced security consultant in the commercial security world as well as within the highly secure networks for the Department of Defense (DOD). He provides expert consulting and consulting management for tasks that include security policy development, network security design and review, vulnerability assessments, penetration testing, intrusion detection, analysis and incident response. Todd is responsible for performing vulnerability assessments on operational networks within the finance, healthcare, and utility industries as well as wireless infrastructures. Todd has been heavily involved in incident response and management as a Security Engineering Lead within Symantec Managed Security Services and as a Consulting and Forensic lead within Symantec Business Advisory Services. Todd is currently working as an advisory consultant within the airline industry supporting third-party risk assessments including risk assessments for migration of Cloud activities.