2007-08
Conflicts of Interest

Introduction:

Eliminating conflicts of interest is, perhaps, the most basic fundamental of an effective security program, and yet few organizations today have even the most basic sort of requirement that the CISO be independent from the CIO. This basic problem has and will continue to cripple the ability to have an effective security program.

What is the nature of this problem?

In order to change this situation, someone has to find a way to convince top management to identify the need to eliminate the conflict of interest. Top management usually has a strong desire to combine all of the information and information technology challenges in one management area of control - the CIO, just as they put all financial matters under the control of the CFO. It makes logical sense, but they seem to have forgotten something fundamental. Without adequate independent review or top-level knowledge and attention, this produces a culture of corruption within the enterprise in which the CIO is all powerful with respect to information and technology.

The good part of this is that the CIO can get anything done that they want to get done. They have to argue to get budget, but they can do what the like with it. All of the checks and balances on power are under their control, so they can do as they like as long as it doesn't unduly interfere with someone else at the highest levels of power.

CIOs in large enterprises typically remain for only 18-24 months. As a result, they prosper when they spend as little money as possible and generate progress that won't come back to hurt them in that period. If they leave a mess for the next CIO, it's no problem. Their goal is to avoid or cover up major security incidents for an 18 month period. So they take risks and cover up failures. The CEO is almost never even told of such incidents because the CIO has the capacity to cover it up because of their control over the only people who could report it. We have seen this happen in scores of cases.

How can this problem be solved?

The only person who can solve this problem is someone who is higher than the CIO in the business hierarchy. That is usually the CEO. Unless and until they take a proactive position and move the CISO out of the control of the CIO or take some other similar measure, the problem will not be solved. But unless you are the CEO and are reading this, how will you ever find out? If you are a CISO, what can you do to let the CEO know?

Letting the CEO know

Unless and until the CEO has detailed knowledge of the security failures in the CIO's area, the root organizational causes for those failures, and the business consequences of those failures, there is nothing they can do to change it. Even after the CEO knows of such problems, they will most often tell the CIO to fix it and the CIO will tell whoever told the CEO to never do it again – or fire them.

This puts the ethical security professional in a bind. The code of ethics of most protection professionals does not codify the protection of the public (or shareholder's) well being, but the code of ethics of most of the engineering professions do. Professional engineers, who are certified or licensed by governments, have leverage in asserting professional responsibility and are rarely overruled by management on technical issues such as the strength of a load bearing wall or the proper gage of wire for a building. When they are, they are faced with an ethical choice that often involves peoples' lives. Most, will refuse to compromise safety. Replacing the engineer will only get more refusals and whistle blowing. But in the protection profession, there are few, if any, mandated standards for protection, except for internal government programs. No professional certifications or licensing is mandated to be a security professional. And protection professionals who work for the CIO and refuse to yield or tell the CEO what's going on are typically fired and replaced by someone – anyone – who will do what the CIO wants.

The ethical bind is really quite straight forward. You either have to put your job on the line all the time or you have to participate in a cover-up of incompetence or malicious neglect. We lean toward putting your job on the line. We have a saying about security jobs:

"You can't do your job if you're worried about losing it"

On the other side, it is commonly expressed that you can't fix the problem if you aren't there. All you can do is make sure that the CEO finds out about it as you are fired. We don't buy into this. We think you can find a way to tell truth to power without getting fired over it – by recognizing that it is their decision, but your job to make sure they are properly informed to make it.

Conclusions:

You need to find a way to meet with the CIO and the CEO periodically and to make the business issues clear in a manner that maximizes your chances of success in changing the things that really need to be changed.. To do it effectively, you also need to be a diplomat, and you need to form a strategy for change.

Copyright © Fred Cohen & Associates, 2008
Specializing in Information Protection Since 1977

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 94:

"Mechanisms of self-serving beliefs"

> *"If you want to believe it you ask "Can I believe it?...[if not] "Must I believe it?" ... preconceptions drive outcomes..."*

When the CEO asks "*Can I believe the CIO?*" the answer is almost always "*Yes*" as long as the abuses aren't so obvious and harmful that they are unavoidable. Unless there is an independent trusted channel for information to come to the CEO, the decisions will always favor the management team in place. The solution is, either an independent CISO or a strong IT-related audit team under the control of the audit committee of the Board.

Page 169, "Separation of Duties" tells us:

> *"Separation of duties is used to assure that individuals cannot cause more than a limited amount of harm..."*

Many top executives ignore this principle for those they work with. It's hard to work with people and not trust them, and perhaps that's a large part of the problem. But separation of duties is fundamental to proper controls, and the CEO that cannot understand and carry this out cannot be permitted to run a public company. That's why they get the big bucks.

Chet's Corner

I have given up on security... again. As a profession, it seems to me that security is always hated, never respected or appreciated, and often feared and fought. And I fight security when I find it obnoxious, inappropriate, or demeaning. When I tell people I work in security, they become cautious towards me. I get the sense they think of me as a computer Nazi. And I hate it. So I have given it up... again. As I will give it up again and again. Because, despite its down sides, it's interesting, and diverse, and challenging, and never boring. But for now, I have given it up...

"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 role as independent outside experts: "*someone to blame it on*".

There are three reasons people hire consultants:

- Not enough time
- Not enough expertise
- An independent outside opinion

The last of these three, we also describe as "*someone to blame it on*" because one of the major roles of the outside expert is to tell management things they don't want to hear and would punish insiders for saying. Independent opinions are just that: opinions. They are generally based on limited time on site, limited access to information and people, and limited budget. They do not necessarily reflect internal decision-making, they can be used to inform without unnecessarily inducing liability, and they can be ignored or overridden without follow-on.

As independent experts, we recognize that we are automatically fired every time we finish a task. But this also leads to ethical challenges. We have been on jobs where insiders told us that we could get a lot of follow-on business if we gave them a favorable report. Our response has always been to quote the statement and cite the source in our report. While many security consultants go along to get along, this has never been our way, and this is precisely the sort of conflict of interest that must be avoided if security is to be balanced against other business needs rather than the personal ambitions of the powerful CIO.

Mollie gets the last word in

Traveling the World when you are young gives you perspectives that you will use for the rest of your life. That's what my parents told me, and I guess it's true. Meeting new people, learning their culture and how to interact with them, and helping to dispel any of their misimpressions about where I come from are all very important for the long run.

Still, the road takes its toll. So far away from home, and only the Internet to connect me to my family, it gets lonely at times. Still, new friends help a lot.

Copyright © Fred Cohen & Associates, 2008
Specializing in Information Protection Since 1977