Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

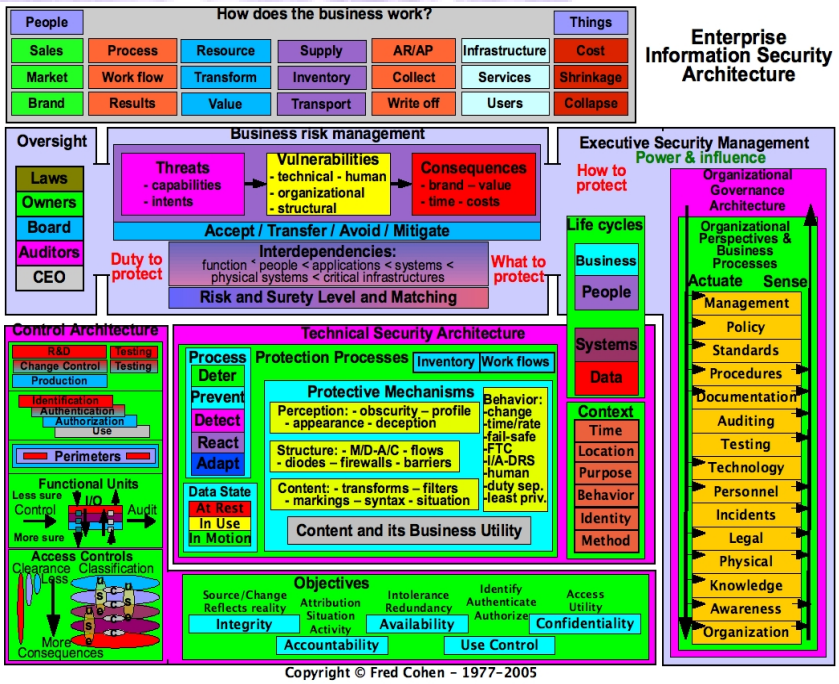
The difference between responsibility and control

In providing information protection, people within an enterprise have responsibilities defined by governance. But they also have only limited control over what the enterprise does. A reasonable explanation for why protection fails to meet management goals is that the people who are responsible for protection, at all levels, don't have or exert adequate control to affect the desired outcomes. This difference between responsibility (R) and control (C) is at the core of how and why protection fails, and is one of the least understood and least measured quantities in protection today.

How can/do we measure R-C?

Many assessments in fact produce measurements reflective of the difference between R and C. For example, the methodology used in information protection posture assessments has rated organizational governance architecture from different perspectives using a {low medium, high} or numerical ranking approach with a relatively small number of values for each of a set of perspectives. In effect, such rankings assert that a particular level of R is desirable and that a particular level of C has been attained.

A more advanced form has been produced using the notion of oversight to define a set of responsibilities, the notion of control architecture to define the metric space for assessing technical controls, organizational perspectives to define the metric space for assessing operational activities, and a risk management framework for turning the duty to protect into decisions about how to protect. All of these have feedback at different rates, which in turn drives measurement.



Losing control

Enterprises often start with a high degree of control by top management, because they often start with one or two individuals who literally make all of the decisions and do everything that is done. But any organization with more than a few people involved will necessarily delegate responsibilities and, in doing so, reduce control by top management in the exchange. While the level of control involved in very small organizations may seem ideal, in the information protection arena, control usually includes doing a wide variety of things that require

specialized knowledge, training, skills, and ongoing effort. Very few small organizations have the set of knowledge, training, and skills, and the resources to apply ongoing effort to the level required to maintain tight control over substantial amounts of information. Larger enterprises may have more control because they can afford the set of knowledge, training, skills, and time required to maintain that increased control.

But of course, that's not always what happens. Growth tends to generate rapid changes, and rapid changes are, in most cases, at least a little bit out of control. People make rapid decisions with less information than they might like to have, and take risks to attain high growth rates in exchange for the rewards that those growth rates produce. As they grow, even if the growth slows down, they may forget about all of the things they stopped doing in order to get to where they are, or they may have never known about all of the things they should have been doing to provide proper control, perhaps because these things were implicit in their decisions when the organization was small, but the growth resulted in delegation, and the delegates did not have the same implicit knowledge and understanding as those who used to be in control.

Another path to loss of control is seeming improvements in efficiency. Reduced cost per unit of output almost always seems like a good idea. Since controls have costs and don't directly increase output, reducing controls always seems more efficient, in the short run. Responsible parties make decisions to reduce control, sometimes without even knowing it, perhaps because they don't understand the indirect effects (sometimes unintended consequences) of their reductions in control, and perhaps because a future possibility seems less important than a present imperative. If you will go out of business in a few months unless you reduce costs, it seems to make sense to stop strategic planning directed towards events 3 years out. And if you get a hefty bonus for another 0.5% net next quarter, the company is telling you to stop doing anything that could produce longer-term growth and profit. Accept any and all risks for that gain, because that's what the bonus says.

So that's how we get increasing loss of control and gaps between responsibility and control. This gap can be measured, but only if management chooses to measure it. The measurement itself is problematic for management in that it puts them on notice, and then they have increased responsibility and liability for the gap. To the extent that they choose to retain or increase the gap, they are making risk management decisions and those have implications. But ignorance is bliss in this regard, unless regulatory mandates, shareholder law suits, or the inevitable business failure comes along. But diligence is not hard to attain through officious means, and all you need is a vendor who is willing to tell you everything is fine in exchange for a hefty fee, and then the risk has been mitigated. Ignorance is bliss, there is no gap, and we are closing it at a prudent pace.

Regaining responsible control

Just because you don't control everything doesn't mean you're being irresponsible. For example, ceding control for commodity items that are readily replaceable in the market and can be bought for less than they can be made by you is generally a reasonable approach. ISP services to transport data, for example, are commonly outsources, with higher reliability gained by redundant paths and service providers. In a stable information economy, this works out well, assuming that there is enough of a governmental presence and stability to assure

continuity. And even when this gets a bit dicey, there is a competitive environment to consider. Paying far more for increased reliability under unlikely conditions may gain a competitive advantage for a short period of an outage, but those who do it less expensively will gain financial advantage day after day, and unless things go bad in a hurry, the net effect of taking those risks may put you out of business while they prosper. That is the nature of risk management. You can also be on the outage, and if you can secure enough of an advantage when it happens, you might put them out of business. And of course, when it is to your advantage to have such failures, there are motives to induce them. After all, another way to make the quarterly net is to increase gross sales by a convenient outage of your competitors.

The key issue in closing the gap between responsibility and control is knowledgeable decision making. When ignorance is bliss, the gap between responsibility and control tends to be high. As resources are spent gaining knowledge, the knowledge gap closes, and as better decision making processes are put in place, the gap between responsibility and control tends to reach a reasoned equilibrium. But of course, the more you spend on gaining that knowledge, the less you have to close the gaps. So spending without limit on making better decisions is also usually a bad decision.

Why we look at consequences first

The solution to how much to spend on making better decisions, while not optimized (it costs too much to optimize the process in many cases), seems to come in the sequence of risk management steps. While the structure of risk management is often couched in terms of threats exploiting vulnerabilities to induce consequences, risk management should normally proceed in a different sequence. Start with the consequences, and for those that are high enough to justify it, look at the threats. Only after you understand these things, and for consequences with threats justifying the effort, should you examine the vulnerabilities. Of course to get at the consequences, you will need to understand the business, and that means business modeling, in terms of identifying the critical information needs and, from there, the likely consequences of loss of control.

Responsibility tends to be divided among people in large organizations. This means that in order to create a viable business model for understanding the gap between responsibility and control, a basic understanding of the business has to be built, and that has to be built and augmented to the level of detail required to differentiate consequences by talking to the people who are responsible for the business functions.

Summary and commentary

On most of the information protection assessments I have led, client personnel ask me, often in a doubting sort of way, why I need to talk to various people like the head of HR, a sales manager, a receptionist, or a facilities manager at a non-data center facility. I explain that in order to understand what's important to the business, I need to understand how the business works, and in order to understand how the business works, I can't just take the technologist's word for it. I have to talk to the people who do the jobs and understand how the lack of control changes the way they get work done. And a large part of the reason I have to do this is because within many enterprises, they don't. Closing the gap between responsibility and control means that those who are responsible must take control, and that means knowing what is going on and why. And that's what a good executive does well.

