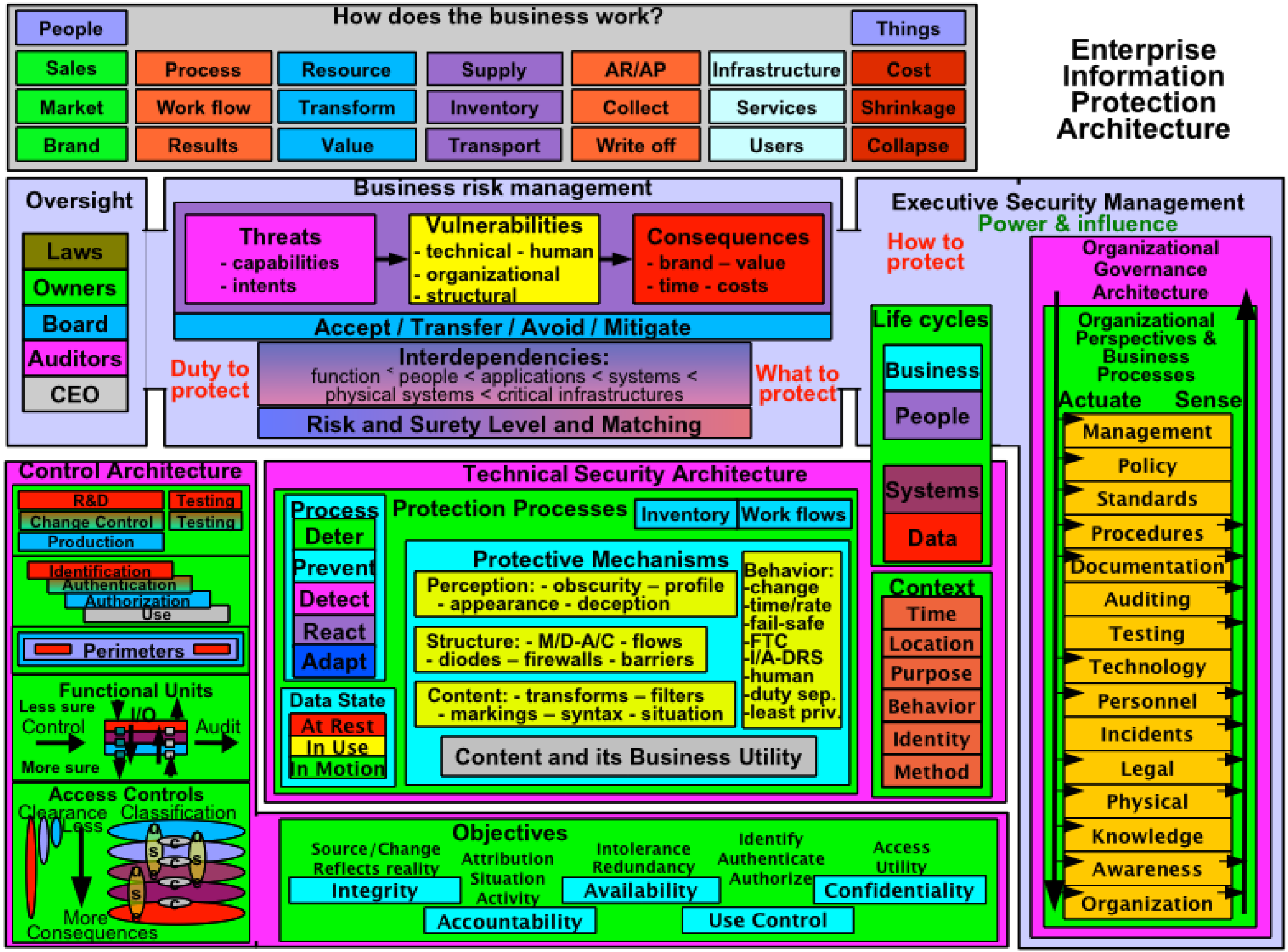
Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our new combined Analyst Report and Newsletter

Enterprise Information Protection – It's about the Business

It seems so natural and fully integrated into the way I approach things that sometimes I forget that not everybody thinks of things in this way. Sometimes it helps to remind myself and everyone else. So this is my periodic reminder. In Figure 1, you see the model of enterprise information protection architecture that I use on a day-to-day basis for my work, my clients, and my students. It has been updated lately to add one item, and at the all.net Web page, you can get a drill-down into the model be selecting “Security Architecture” and picking whatever you are interested in from the clickable version of this picture.



Copyright © Fred Cohen - 1977-2008

Figure 1 – Enterprise Information Protection Architecture on One Slide

What do I mean – about the business?

When I say it's about the business, what I mean to say is more than a mantra to satisfy the people with the money. It goes to the way you explore the space and think about issues. If you are thinking about technology, you are not thinking about the business. If you are thinking about money, you are not thinking about the business either. Even though money and technology are typically critical to running a business, the business is not just money or technology. I'll go out on a limb here and identify that a business is a set of activities that are carried out in order to provide a set of customers with something they value in exchange for something of value that they provide to the business. Information technology, as much as and perhaps more than anything else, is a tool that helps the business serve customers and exchange value through the use of content for business purposes. The content is the meaningful stuff associated with what we usually call information, regardless of its form, location, mechanisms of use, or other properties. This usefulness of content, or as I call it, "utility of content" is what the business gains by controlling it in different ways. The business can also lose the utility of the content, or even get negative utility out of it, if it is corrupted so as to be unsuitable for the purpose, unavailable when needed, leaks to those who shouldn't have it, cannot be controlled properly as to use, or cannot be accounted for properly. I call the process of bringing certainty to the utility of content "assuring the utility of content". That then is the task of the enterprise information protection process and architecture – to assure the utility of content.

The purpose of enterprise information protection is to assure the utility of content.

When taken from this perspective, it becomes clear quickly that in order to assure the utility of content for an enterprise of substantial size, the information protection effort has to become systematic and apply automation in various ways in order to be reliable and cost effective. While we have a great deal of automation for technological aspects of information protection, that technological support is largely lacking when it comes to the non-technology aspects of enterprise information protection. For a good example of how true this is, look at our analyst report from February of 2007. While technology to support technology is all fine and good, the goal should be for technology to support the business. Of course it's easier to apply technology to other technology than to a business because all of the other technology is in the same form – bits stored in computers – readily available – easily manipulated – certain to have known values – and easy to compel cooperation from. But businesses are, with few exceptions, not just piles of bits ripe for the picking and manipulation. Most businesses are processes designed to exchange value for value. And that's where we lack adequate attention and understanding in most cases.

I will continue to focus on how we accomplish the business focus of information protection over future issues, but for now, I will ask you to simply look at and think over the areas with the gray underlying background from Figure 1 and consider how the business has to drive the protection approach and mechanisms.

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 Security Governance Architecture Reviews.

> *One of the most common functions we provide for clients is the review of their enterprise security governance architecture. This generally comes in the form of a current status review with urgent, tactical, and strategic roadmaps that address desired changes over different time frames.*

Unlike a technical security review, a governance review focuses on the business side of the protection function and considers how the business functions required in order to make the protection program effective is working and how it should change to meet the governance challenges of today and tomorrow. While technical security is, of course, critical to the execution of protection programs, any program that is going to work, also has to have management systems in place, executive oversight and buy-in, an enterprise measurement and feedback systems in place, linkage to regulatory drivers like Sarbanes-Oxley efforts, power and influence strategies in place for representing the protection function in the context of enterprise operational and governance needs, integration with the risk management function of the enterprise as a whole, and any number of other things.

> *In one recent study, a client asked us to look at enterprise encryption efforts with an eye toward understanding how to move from their existing, largely uncoordinated, evolution-driven approach to handling encryption toward an enterprise-wide approach. We applied our standard methodologies to understanding enterprise governance in the context of the issue of encryption and helped them develop a comprehensive long-term approach that they could live with.*

Upcoming Events

March 6, 2008 – Cornerstones of Trust (ISSA and InfraGard) – Fred Cohen will present "*Enterprise Information Protection – It's About the Business*" - A talk on how business modeling, inventory, and work flows are key to the integration of information protection in to the business and how they can be built up and applied to help create a mature and normalized enterprise information protection program.

Some time in March: New Book Released - "*Challenges to Digital Forensic Evidence*" will be released for sale to the public in March. This book is the first of its kind, examining how the seemingly perfect evidence provided by computers and other digital technologies can be challenged in legal cases and how to avoid these sorts of challenges.

April 7, 2008 - MiniMetriCon will be held near the RSA conference for the security metrics community to work on issues surrounding measurement of security. FCA is a sponsor and Fred Cohen will be participating in the discussions.

April 11, 2008 – RSA conference – Fred Cohen will present "Improving Security Decisions" to the management track. This will show how tools help executives better understand security-related decisions and how decisions can be clarified and justified to make business sense.