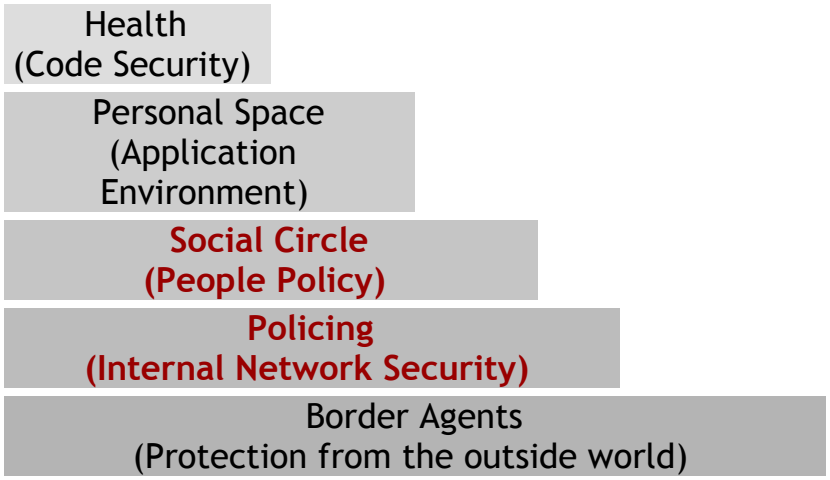
# The Application Security Pyramid - Policing and People Policy

Posted At : April 13, 2006 1:31 PM | Posted By : Mark Kruger
Related Categories: Security

This post is a continuation of a 5 part series on security called "The Application Security Pyramid". The introduction introduced a new metaphor for dealing with security that loosely mimics Maslow's heirarchy of self-actualization. In Part I I discussed the importance of "border patrol" technology to safeguard your network. This post will deal with internal Policing and People Policy.

It's not enough to have effective border agents to feel safe. We also have to have effective policing inside our borders. After all, there are people here who are forced to work for the post office and they need watching. A system of policing and civil services keep us operating in safety and harmony with one another. This is the next two blocks on our pyramid - internal policing and people policy.

- Intro
- Part I
- Part III
- Part IV




Security *policy* maintains the boundaries on a network - or at least that's the idea. In fact most IT security professionals proclaim that *internal users* are the biggest threat to the security of any company and probably your application as well. When it comes to security policy users tend to see it as an unnecessary inconvenience. They take the attitude of the infamous, evil, and extremely funny Captain Barbosa played by Geoffrey Rush in "Pirates of the Caribbean". When asked to adhere to the written-in-blood pirates code he responds, "It's more like a guideline actually".

The problem is ably laid out in this short journal article by C.J. Kelly titled securing data when data is everywhere. She rightly points out that data has a natural tendency to proliferate by morphing into different forms and being copied, emailed, printed and otherwise reproducing like a crowd of French bunnies in the hutch back of Notre Dame. Regarding controlling security she states:

> "Ideally, IT security would understand how people work, what they need and what

> they are trying to accomplish. Then we could get in front of any effort to manipulate data to make sure that something like an Access database has the proper security controls in place. That's not usually how things go. Generally, data is saved in various formats and then e-mailed, transferred, shared and printed. Afterward, the original data has morphed and has numerous owners and locations."

She goes on to recount a particular case of data from controlled systems that was showing up in access databases because users liked the convenience for query and reporting. She recounts her efforts of trying to find a way to secure access databases and ends with a plea for any suggestions that folks might have. She might as well have asked for suggestions on building a perpetual motion machine or on what women actually want.

Still, having a *security policy* is a cornerstone of network security. A security policy should be a published set of guidelines for users to follow. This policy is like the police in our analogy - an arm of the law. I like the idea of not making such a document specific to any technology (as in "you must use browser A, B or C"). Rather it should be behavior based and focused on the goal of security and data protection. A good security document handles the *goals* of protecting data from unauthorized access and data corruption. It should be flexible enough to shift as technology changes without giving up the essential objectives.

The site **ruskwig.com** has some decent security templates. Some of the templates are targeting IT people and are necessarily specific and technical, but some of them are targeting regular users and they are written to be understood by them. This template on **user responsibilities** is a good one. It is succinct and to the point. It has a little bit too much stick and not enough carrot about it, but all in all it would be hard to misconstrue it's meaning.

Unfortunately, many companies create security policies for the purpose of passing an audit, not for the purpose of controlling and managing access to applications and data. That's why so many of them are filled with buzz words and acronyms. They tend to impose strict limitations in certain areas like domain access, password policies, file system encryption, VPN access rules, and email filtering and monitoring. By sheer coincidence these important areas are all areas where an auditor might be prone to look.

Security policies often don't address things like data morphing - where something from an online secure page is copied into a spread sheet for convenience and emailed to someone else, who copies it to Access and emails it to a third person, who copies it as text into his email after posting it on his blog. If the user in question has access to Excel or Access, how are they going to be prevented from using it for data to which they also have access? More to the point, how are you going to communicate to them that using tools in this manner is a risk? After all, you gave them these tools, right?

While policing and policy is important, it doesn't have quite enough of the human equation in it. In fact, many security breeches occur through *social engineering*. IT is often not equipped to deal with "people policy". Remember, people have a natural tendency toward optimism and a bent toward convenience. If rules are too stringent they are circumvented with the attitude of "what could happen?". In most companies there are 2 parallel paths, "our policy" and "the way things actually work". So it is important that we deal with people as people. We can stomp our foot and insist on a

police state, or we can work to collaborate with our users and develop a community effort at "keeping our company safe".

**Some Ideas for Policing**

In some communities that struggle with crime the idea of *community policing* has taken root. Community policing tries to soften the adversarial relationship between the police and community by treating policeman as members of the community. This approach has shown some merit because police take ownership of issues that belong to "our community" rather than seeing the "men in blue" against the world. In return, community members have a framework for a higher level of trust. Policing becomes a collaborative effort rather than an intrusion.

In the network an effective security policy is one in which the IT staff are seen as collaborators and not as *enforcers*. Too often IT is seen as an obstacle to overcome rather than a facilitator. There might be many reasons for this, but here are a few:

- IT sometimes has a reputation for elitism and attitudes of self-importance. IT tends to look down on other departments and see themselves as power brokers. They expect folks to approach them Hat in hand as supplicants when they want something done. This is definitely the tail wagging the dog is the majority of cases. IT is an internal service organization. Ideally it should treat other (*revenue producing*) departments as customers who pay the bills.
- Many security rules seem arbitrary. If your security policy is going to make sense it cannot just be written and posted on the intranet like Luther's 95 theses nailed to the Castle Church door. IT must do a better job of explaining why the rules exist. It must "sell" it's customers on the value of such rules and strike a conciliatory tone.
- There is a lack of clear communication. Too often IT breezes in and fixes problems that are "too technical" for the user to grasp, which is a catch phrase for the capture and retention of knowledge (and knowledge is power). Finding IT people who are good communicators is an important first step.

As in so many things in business and in life, healthy relationships between people can lead to positive results. Alas, even if all of these things are resolved and you have a clear policy in place clearly communicated and everyone on board and happy, the truth is that internal policing is a *running battle*. People do things that seem thoughtless to us - but don't raise any red flags with them.

For example, Mitch from marketing brings his wireless router from home so he can browse the web on his laptop from the café downstairs. It seems clever to him, and indeed it is. He's just the sort of innovator you might want at your company. He has no idea he's painting a big target on your network. Sally Sales Girl loves those little USB key fob thingies. She can copy her whole "my documents" folder onto it and do some work at home in the evening. She's aggressive and dedicated - a benefit to your company. She's not aware that your company data is now at the mercy of her possibly non-existent home network security. Victor VP can't remember his password so he writes it on a sticky note and pastes it on his monitor. It's just a convenience to him. Never mind that a snap shot from a camera phone could give anyone within site of his office door a window into his corporate world.

It would be easy to weep and wail and gnash our teeth and decry how these things shouldn't be this way. That would have no effect. In fact, just like the real police, we

need to recognize that ongoing education and enforcement is part of the job. Mitch, Sally and Victor will always be a headache - but that doesn't mean we can't love and appreciate them. If you think I'm settling for an attitude of resignation to the inevitable, you are right. I believe that no amount of education and policy will ever take away from the fact that part of IT's job is cleanup. Just like civil services (fireman, garbage collection, national guard) we are sometimes called in when something bad happens.

So what have we learned? Internal users are as much of a threat to your application and network security as external users. A policy must be written, communicated and enforced. Collaboration and "selling" your policy are keys to making it work. Some failures are inevitable and cannot be prevented. Having a "people oriented" policy will do much to improve your overall effort.

In our next post we will talk about how to secure the system that belongs to your application.