2007-04
Information Content Inventory

Introduction:

A client asked me what to put into an inventory list I asked them to make of all of the content they held. It occurred to me that while I knew what I wanted to get from them, most of the standards I was aware of had little relevant information on what to put into such an inventory, even while some of them require that you have one. So I decided to try to look up the answer on the Internet. After that more or less failed, I decided to write this article.

So obvious you forgot to do it

It seems like it is so very obvious that in order to control anything you need to know what it is that you have. But it is not that obvious. Common sense is not that common. Few of the enterprises I have worked with have an explicit inventory of content they control, link that content to owners, associate it with risks, and classify it. Yes – it is so obvious that we tend to forget it. How much did I find on it from the Internet? I found one decent article from 2001 and the fact that several standards call for one. No surprise given that I already read the standards.

Yes – I have one

I always ask myself if I have done what I ask my clients to do. If not, I do it first or determine a good reason that I should not. In my case I have a more or less hierarchical system of controlling content. It is in a distributed directory structure with a naming convention and organized by content type. This yields an automated inventory of sorts but it doesn't scale well and cannot reasonably work for more than a hundred people. I have seen it break down at client sites with only 20 people. But it does work for me.

My implicit inventory associates content with ownership, has naming conventions, puts like content together, values content based on consequences of protection failures, etc. It is rudimentary, but with a one second request and a few minutes of execution, I can come up with a comprehensive list of all content in my possession, all source programs, all documents related to whatever issue, all emails with a given individual, organization, or containing specific character sequences, and so forth. I can do the same for archival data, after removing it from the safe or getting it from a remote storage location. I have documentation to support what is encrypted (all of it other than that physically secured), the protective measures surrounding it, and so forth.

But what if you are bigger than this?

The bigger you are the more you need an inventory control system that handles your information assets. While for small shops inventory can be an integrated part of systems operations, for most larger shops, things get out of control too quickly and become unmanageable if they depend on users systematically putting things where they belong.

I learned filing and inventory control over records from my uncle's law firm. They have hundreds of thousands of cases with physical files that they have managed for scores of years. When I helped automate their processes we built a scalable system that, in addition to producing authoritative and unalterable electronic records of all of their actions, also tracked them to paper records and tracked the paper records to physical locations. It was far from perfect, but the time to find a physical file went from hours to minutes with the new system, the paper records were needed less of the time, and over time, paper records became almost completely unused in select portions of their practice. This is all traceable to the creation of an automated system to control information content inventory over its entire lifecycle.

You can do the same thing for tracking enterprise information assets and mimic all of the processes required for checking content in and out for relatively little cost. The result will be a lifecycle approach to control of content that will allow security functions to proceed in a systematic manner with traceability as business records and regular processes applied to them. But it may not be as easy for you as it was for me. Law offices have structure, everything ties to cases for clients. Practices have been around for a long time with established procedures that are followed by workers on a regular and repeatable basis. Structuring your records also means structuring your business. Your business processes have to work in order for your records management to work, and inventory is usually the first step in this process. The bigger you are the more you need a systematic approach to controlling assets.

Conclusions:

Hopefully I am preaching to the choir. You cannot effectively control what you don't know to exist, and for any substantial enterprise, this means the creation and proper maintenance of an inventory of information assets.

(1) It is obvious and yet often forgotten.
(2) You will have to create your own standards.
(3) Get your assets in an inventory today.

It's just common sense.

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 19, section 2.3.4.8 we present the easy as slices of pie:

"Shorting"

> *"The vendor ships less than the quantity specified but bills for the entire amount. If the target doesn't do reconciliation the vendor makes a bit more on every shipment. Targets often end up calling this part of shrinkage when they cannot trace it to a specific cause."*

Section 6.1.4.4 (page 174), "Manipulated Goods" starts out by stating that:

> *"Once goods leave inventory there is little that can be done about them being manipulated..."*

It should be no surprise that inventory is key to preventing frauds and any number of other mishaps whether in physical or informational form. Inventory of things of value needs to work across the entire life cycle of the content – whether it is a physical asset that arrives from a vendor or an information asset that arrives via a file transfer protocol. Assets need to be inventoried, and even if they are not fully valued for whatever reason, they need to be tracked in order to prevent anything from simple mishandling to loss of utility.

Tracking information assets creates a lot of issues for enterprises. For one thing, they follow the laws of information physics rather than physical goods physics which means that, for example, I can still have them even though they have been stolen... think about it. On the other hand, the cost of tagging physical goods, even in the era of RFID tags, is non-trivial while the cost of tracking information as it moves around a system or network can be relatively low cost if embedded in the controls of the enterprise.

Many companies now track select information inventory at boundaries using systems that look for known internal content, while many trusted systems tag everything and watch tags to limit and audit movement. Whatever view you take of it, tying information content to inventory is a key issue.

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 creating information security inventory and using it as a foundation for a metrics program:

When we create metrics programs for clients, it's usually as a side effect of an assessment or other similar work. One of the first things we ask is what content, systems, people, and business units are out there. There is rarely more than a simple inventory of systems and, if identity management is in place, users authorized to use them. So we often have to generate the list of all the content they have and its properties. Here are some of the things we often need in a content inventory for risk management:

- A list of data fields within records so we can determine content types (personal information, credit cards, financial data, etc.)
- A list of jurisdictions that apply to the content and it locations (so we can figure out which laws and regulations apply to it).
- Contractual obligations (so we can analyze the contracts for protective requirements).
- How much of it is there? This helps identify what protections are reasonable.
- Ownership (who owns it for the enterprise and who owns it legally).
- Consequences of loss of integrity, availability, confidentiality, accountability, and use control (so we can do risk management).

Since we couldn't find any tools to help us do this, we developed survey tools to gather details from internal owners. Here are some of the tools we have created to deal with these issues as part of our Surveyor platform:

- RiskLevel – gathers content inventory and risk level information.
- SecPerf – security performance indicators.
- TechSec – technical security components.

These tools help us to create and, over time, track information security inventory. RiskLevel covers content and its risk features; SecPerf covers the management process; and TechSec covers technical security components. Measurement over time also leads to the rudiments of a security metrics program.