All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Security Inventory

Some years ago, a Verizon study showed that most leaks of confidential information from cyber attack involved content or systems not in the security inventory.

Of course it is stupidly obvious that if you don't know you have it you are unlikely to properly control it. But on the other hand, how many of us have a good inventory of everything related to cyber-security? Do you? I know mine is far from perfect.

But what is a good cyber-security inventory?

A cyber-security inventory is (1) an inventory and (2) one that's helpful in dealing with cyber-security issues. But that requires some more in-depth consideration.

I always check with the standards of practice first, so let's look what the peer reviewed published version tells us:

- Inventory of {Hardware, Software, Content, People, Uses, Linkages} is used for {business understanding, modeling, analysis, simulation, risk management, organizational purposes, measure coverage and completeness, control architecture linkage} and is {up to date, accurate, granular} to the required level - using a {unified database, combination of databases, set of disparate repositories, information in peoples' heads}

Of course it details the circumstances for each of these sets of sequences based on risk and program maturity. But let's drill down from there…

What and why?

Hardware is pretty obvious – or so it would seem...

> Physical devices are often already inventoried in the asset management system.
>
> **However**, in today's environment, much of the hardware in use is mobile devices not owned or in the inventory of the entity whose content/systems are supposed to be protected.
>
> And even for hardware in a physical location, inventory of cabling, cabinetry, and similar things is often not kept at a granular level. That's because the cost of tacking it is probably not worth the consequences in terms of capital issues.
>
> > For example, when we expense a purchase, from a standpoint of accounting, it is written off and has no residual value. So there is often no reason to keep it in inventory.
> >
> > Similarly, after inventory items are written off, they have no value in tax savings so they fall out of inventory for that purpose.
>
> **But from a security standpoint,** even items with no tax write-off value may store, process, communicate, or otherwise be critical to content or operations. Which is to say...

It’s about the utility

We cannot yet inventory all Items for all purposes at all times with perfect accuracy at the finest granularity in a distributed database. And we likely never will be able to. Attackers understand these issues and exploit them. For example:

- A failure to properly inventory content in physical items being disposed of leads to not applying proper resources for destruction of contained content.
  - So attackers dumpster dive, find residual data on media, and gain unauthorized access.
    - Suppose we inventory all items of content and hardware and linkages that associate content items with all hardware items they have entered.
      - Now we can determine that the hardware item at one point contained a content item that inventory indicated something about.
        - But what did it indicate? And is that indication still relevant? And what does that indication imply in terms of processing of the hardware for disposal?

Imagine tracking all of this for every item of data and revaluing everything over time to do analysis for decision support.

- The zip code of my address in Coopersburg, PA is likely (now) personally identifiable information (PII). It wasn’t then because there was no such thing.
  - My inventory of everything had to be updated to determine that every zip code everywhere was now PII in relevant jurisdictions (which also changed over time).
    - My tracking of disks that contained files that had that zip code has to include details of what location in what disk sector contained the zip code so that the residual data after the files containing the content were deleted is needed to determine when the item went out of inventory from there as it was overwritten by another file.
      - My tracking of backups indicates the content still resides on a tape that got the data from a printer queue during backup in 1988, because the tape was only partially overwritten in 1992 for another use.
        - The cache memory on the system supporting tape backups was stored on disk when it was temporarily paged out, and the system subsequently crashed before we could confirm proper deletion.
          - And on and on

Inventory is a key to properly processing items through the security operational controls. But operational controls have to have some reasonable approach that mitigates the need to have this level of granularity for inventory on all items of possible future interest.

So there is a necessary integration of operational controls and inventory at an architectural level to assure that reasonable and prudent steps are taken without going to ridiculous extremes or putting items at unnecessary risk for the rewards of having those items.

An OT example of utility

Suppose I run a power generation station. It has a water supply that turns motors that produce electricity. We monitor the voltage and current outputs and control the flow of water through the system by automatically opening and closing physical barriers to produce the desired power, support maintenance, and so forth.

To do this, we have a specific set of hardware, software, content, people, and uses of the cybernetic system. These are linked together by the operational design of the system, so that, for example, only properly trained and certified technicians are allowed to do maintenance on motors they are certified for and authorized to maintain, they are authorized to shut down the water flow to a generator they are scheduled to work on, and they or their supervisor are the only ones authorized to restart such water flow after they stop it.

The inventory plays into this because all of the items involved have to be managed by the systems involved in order for the mechanisms to perform as desired. For example:

- Inventory of people includes the supervisors and technicians and must provide information on their current level of training and certification for the relevant pieces of equipment involved in the maintenance operation.
- Inventory of the hardware includes the equipment being maintained and the devices associated with the operation and must provide information on the part numbers or similar identifying information to allow determination that the maintenance technician is trained and authorized to maintain this particular piece of equipment.
- Inventory of the uses includes the uses associated with maintenance and must provide for test regimens, stopping and restarting, shutting down flows, opening and closing doors, and so forth because these are required for the maintenance functions.
- Inventory of software is required because different software elements execute the uses identified for maintenance and is necessary because uses are only authorized by specific people in specific circumstances.
- Inventory of linkages is required because the linkages between the hardware, software, people, and uses must change over time to reflect changes in training, certifications, positions held, and operations authorized, circumstances, etc.

So in this case, inventory of Hardware, Software, People, Uses, and Linkages is used for business understanding, modeling, analysis (e.g., to track the overall system and its operational efficiency), risk management (e.g., only properly certified and titled people can undertake specific acts), organizational purposes (e.g., to determine when we need to retrain or re-certify more generator technicians on what pieces of equipment), measure coverage and completeness (i.e., make sure we aren’t missing something important here), and control architecture linkage (e.g., not allow someone else to turn on a generator while the technician is working on it) and is up to date (e.g., you are still certified for this), accurate (e.g., you are working on the generator), granular (e.g., we aren’t shutting down the entire generation plant every time we work on a specific generator) to the required level - using a variety of different combination of databases and set of disparate repositories.

In this case we decided not to include an inventory of every wire in every winding of every generator. But we probably do want inventory control over the wiring for the safety interlocks.

Just the beginning

Of course this is not a comprehensive list of the inventory items for cybersecurity for this facility. It is just an example to get a sense of the sort of things involved in a cybersecurity inventory.

The only way to get a reasonably complete set of these things is to understand the facility and how and why it operates, the protective requirements and how and why it operates in the context of the facility, how these requirements are met (e.g., are there physical interlocks in the safety system as well as logical interlocks in the control system and how do they interact), and in that context to identify the necessary items worth inventorying to assure that the process operates as desired to within the desired level of certainty for the identified consequences of failures. From there you can then start to do an inventory and start using it to track what you are doing and make better decisions.

It’s the BOM

Even the longest journey starts with a single step. As a generic starting point toward a security inventory, a good place to look is the BOM. The Bill Of Materials (BOM) is a list typically produced during the design and as part of the purchase and deployment of an operational system. It includes part numbers, quantities, costs (or pricing) and typically does so at the component level for all components within a composite. So a plant with 5 generators, 5 waterways, and a control system will typically have a BOM for the plant that includes or leads to a BOM for each generator, each waterway, and the control system. Each part in the BOM will be labeled (if there are 500 identical set screws, they are probably not individually labeled, but each cable should be associated with a label at each end and have corresponding labels where they plug in). There will also be a list of labels and what they label, typically associated with the BOM of each component and/or the overall composite.

Those darned computer people

One of the things that bothers a lot of OT folks is that the IT folks aren’t generally used to this level of rigor. They tend not to do engineering change orders, track every part, have standard test regimens for every sort of change, re-certify equipment every time there is a change, etc. But those computer people are the ones that hold the databases and spreadsheets that produce the BOM, contain the change orders and supporting processes, etc. these days. So get used to it.

We’ve only just begun

Of course this is not the end. It’s just the beginning. Start with the BOM and work from there is a good plan. But what do we need to add to the BOM? Typically, everything associated with every listed item per its use. And we have to add the people (from the HR database and identity management system), the software (which should be required in but is often missing from the BOM), the content (relevant files, databases, elements from those items, metadata, etc. per the situational need), the uses (often partially available in the rules and roles or similar controls of the identity management system), and then we just have to link them all...

Conclusions

Security inventory is one of those topics too rarely and lightly explored. It usually exists in a disparate set of databases and in peoples’ heads. So let’s get it (all) together and manage it.