7 Pitfalls of TAM

NIyte Software

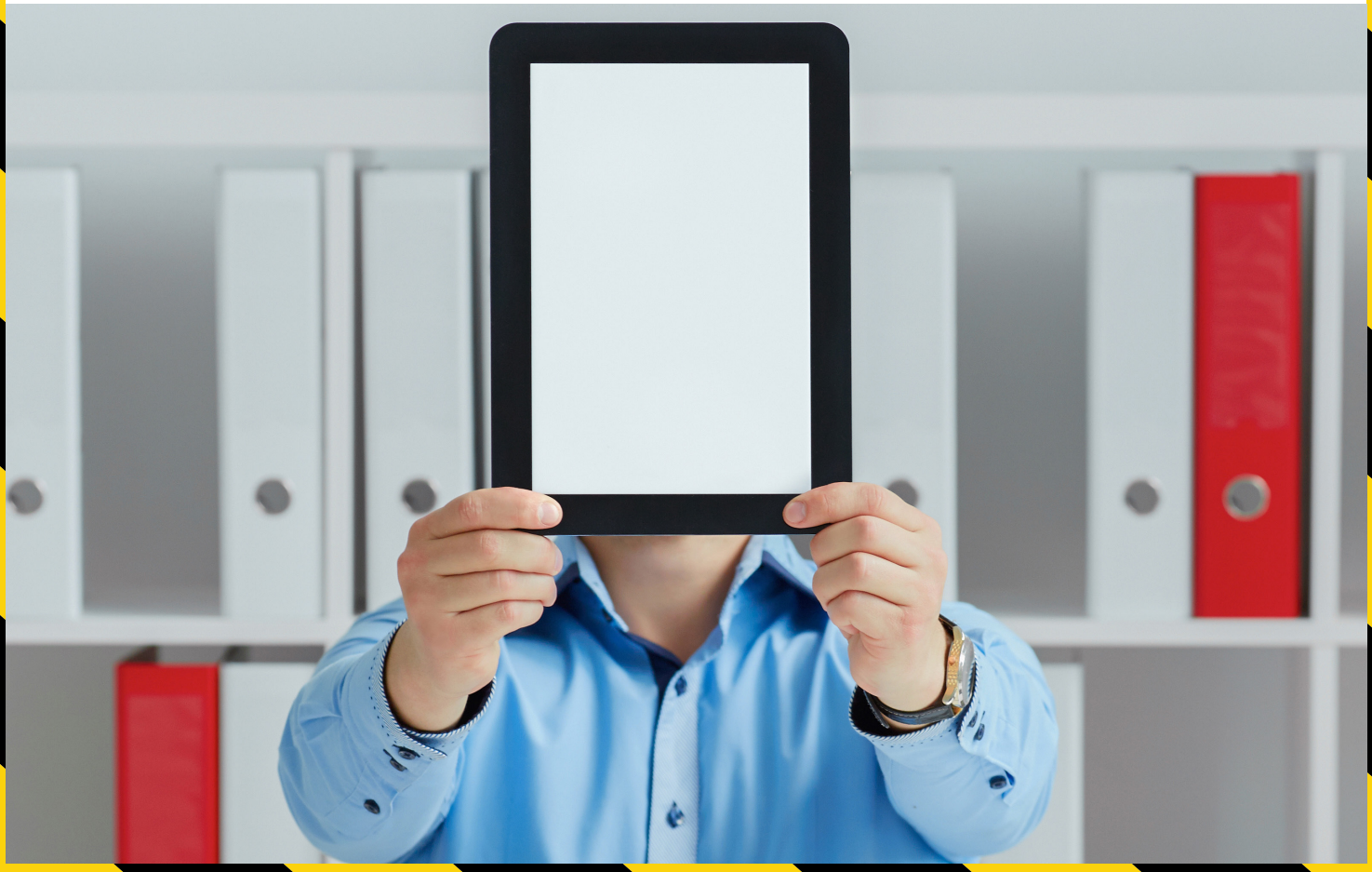
#1 OBSCURITY

Obscurity is the state of being inconspicuous, unknown, or unimportant.

This is thinking your actions or lack of actions do not matter or will go unnoticed. In Technology Asset Management obscurity also holds true for the belief that it won't matter if someone finds out that you are using more software licenses that you are supposed to or thinking that all your firmware and software has been patched with the latest security updates, just because someone said so. Ultimately not knowing if you have enough software licenses, thinking everything is patched, or old versions of software and firmware exist, will matter a lot. You may think you are too small, won't be noticed, or the issue so obscure, but ignorance is not bliss and a sure path to audit or cyber breach.

Solution:

To correct the obscurity missteps you must recognizes and take action getting control of all your technology assets (IT and non-IT). Don't think your company or the threat of cybercrime is to obscure for a Black Hat to poke a hole in your precious little network and wreak havoc. You need to gain insight cognizant of the hardware, firmware, and software that is coming and going on your network continuously. There's a software company that wants more money and will find you are using more of their software than you should because it is easy revenue for them, no matter how insignificant you think you are.



#2 INDOLENCE

Indolence is the avoidance of activity or exertion. Believing that a single static technology asset baseline is good enough is an act of Indolence. Thinking that spreadsheets and CMDB's get updated every time with every change, by every person is a clear misstep of Obscurity, but sitting on your cushioned desk chair and doing nothing about it will land you quickly into a compliance nightmare. Compliance audits, fixed asset reconciliation, SOX, HIPPA, GDPR, "lions, tigers, and bears, oh my" is right! The inventory of assets is continuously changing – hardware, software, firmware, and network connection – and not actively validating the changes is pure unadulterated indolence. Not monitoring and verifying the current state of all assets is a sure-fire way to massive heartburn from compliance audits, security breaches, financial adjustment (a.k.a. loss of budget), and operational chaos. Yes, you start with a technology asset baseline, but ultimately you must be periodically updating it to keep yourself compliant, secure, financially sound, and optimized for the assets in your care.

Solution:
To avoid stepping into the pit of Indolence you need to create a plan, consistent with your IT, Security, Compliance, and Finance policies, to monitor and report on the state of all assets continuously. Implement technology that can consistently monitor and inform you and others changes out of compliance and usage of every asset against the plan. Ensure the technology normalizes the data and analyzes it appropriately for each of the other business systems to which it connects.

#3 PURBLINDNESS

Purblindness is having impaired or defective vision

A Purblindness misstep is different than that of Obscurity. While in case of both you are fooling yourself, here you are allowing yourself to be blinded by systems and technology. Thinking that all discovery type tools are equal will land you in hot water. Most technologies lack visibility across the entire extended enterprise. They may support a limited set of technologies like Microsoft or desktops but lack cross-platform support like Linux, UNIX, and data center assets. These inferior tools do not have the ability to search across all protocols, see assets that are not under management, or see and rationalize various subnets on the network. This instance of shortsightedness leaves you with impaired vision on the assets, firmware, software, and IoT assets running on the network. Your impaired vision can lead your organization to compliance, security, and finance issues as well as potential security or finance issues - and loss of sleep and budget for you.

Solution:

To avoid the Technology Asset Management tar pit, or at least a lot of hot water for yourself, is to implement a solution that allows you to decide what information you're interested in, capture just that and only that. The solution should work across varying protocols, supports Linux, Microsoft, and UNIX, communicate with desktops, data centers, to IoT devices. The platform should give you a complete comprehensive view of all your assets that you're interested in ensuring you do not have holes in your strategy. A good Technology Asset Management solution can deliver hundreds of attributes, as required.

#4 SQUANDER

Squandered is to waste in a reckless and foolish manner

The misstep of Squander is rooted in the belief that more is better, buying more, installing more, allocating more because you don't know how much is needed is just wrong. Buying more software licenses "just in case" is a waste of one of your most valuable commodities - money. The excess software is sitting doing nothing, and you are paying support and maintenance on it too. There might even be some other group who needs it, but you consumed the budget for the year, so shame on you. Not knowing the actual usage of hardware and software leads to overprovisioning. Again, these are assets (money/budget) sitting idle in the off chance that you might need, additional compute, power, application, storage, and or network bandwidth. Before you go writing work orders and purchase requests for more hardware and software assets you should know your actual need. You need to do some serious soul-searching…think, plan, analyze, and then act on facts.

Solution:

The lure to Squander is understandable, you have budget so spend it. You buy health insurance even though you're healthy, but that is because you don't know if and when you will fall ill. To manage your compute infrastructure you buy more, install, more, pay for more on the off-chance you might need more – assets, compute, power, applications, storage, bandwidth, etc. However, with a little bit of discovery, you can figure out exactly who needs what, where, and when. If you have already deftly managed against the first three missteps, you know you can plan and act intelligently with your purchasing and implementation and avoid the misstep of Squander. So the solution is to implement a technology asset management system that can determine what you have, analyze real usage, and reconcile against purchase and SLA commitments. Then tie the asset management system into other IT and business systems to create a closed-loop system to eliminate Squander.

#5 OBSTREPEROUSNESS

Obstreperousness is to be noisy unruly or defiant

Obstreperousness is like the over-beating of drums, while it may get the attention it most likely is drowning out the important message. Implementing technology that is inconsiderate of the network environment, it coexists in, overstays it's welcome and obliterates the very environment it is intended to help is just bad practice. Also, in many of the cases of obstreperous solutions, they are squelched to the point of uselessness or even elimination because they make too much noise on the network. This dismissal of poor behaving technology forces you into the pit of Indolence, working from a static technology asset baseline - remember that baseline - the one that is continually deteriorating every moment - along with your organization's success.

Solution:

While the road in front of the Obstreperousness was full of good intention, look where it gets you. The best discipline to avoid going down this road is to deploy a solution that not only gets just the information you need but does it in a way that doesn't overwhelm the network. To invoke this discipline, it means you must seek out a solution that can automatically throttle its activity, minimize the amount of information you're pulling back (delta changes only) ensuring the solution improves the compute infrastructure performance and SLA's not overwhelming them. This way your impact on the network is as quiet as a library.

#6 AVARICIOUSNESS

Avariciousness is to be immoderately desirous of wealth, money, or gain: greedy.

Are you smitten by the call of Avariciousness, believing the only risks you have in technology asset management is a financial risk? Naivety to other risks will halt your organization's success with fervor and impunity. Allowing cybersecurity holes to emerge on your assets by not having firmware updates in place is a very grave transgression. Not implementing an asset management strategy, allowing assets to go unrecognized, unmanaged, and or not properly accounted for, are all pitfalls of avariciousness. By not implementing a clear and practical asset management strategy you demonstrate your aversion to respecting organizational needs beyond those of finance. Foolishly the endless focus on the pot of gold results in not having a clear understanding of what assets, what versions, what patches exist on assets ultimately depleting the transgressor of time and budget. Although important, the needs of the organization go beyond just money.

Solution:

Overcoming the consumption of Avariciousness is to recognize that preserving money is an important reason to implement useful technology to manage your assets – but it's not the only thing that matters. Having a firm understanding of the hardware, firmware, software, and IoT assets you have coming going on your network reduces your security risks which could cost millions, improves accuracy, efficiency, and transparency across the organization saving hundreds of working hours. Protecting that pot of gold but not seeing the organizations other needs will ultimately put a hole in that pot of gold, due to breaches and failures caused by the lack of a comprehensive Technology Asset Management approach.

#7 PROCRASTINATION

Procrastination is to put off doing something especially out of habitual carelessness or laziness

Many of us suffer from the curse of procrastination, but it becomes a real concern when you believe you can put off the issue of technology asset management to another more convenient day. This laissez-faire attitude may be because of a underlying symptom of Purblindness - thinking you won't be held accountable if software licenses are out of sync - hardware systems don't have the latest patches - or you can't account for where user data is and who has access to it. Ignoring the need to implement a technology asset management solution now is more than a lapse in judgment, and the problem is only going to get bigger day by day. Don't procrastinate, it is just like a dangerous health issue in the human body, you can ignore it for some time, but ultimately it becomes an explosive issue and worse for your organization the longer you wait.

Solution:

Procrastination can come from being overwhelmed by the depth of a situation. It is a form of paralysis and only solved by putting proper controls in place and implementing comprehensive discovery technology to understand what is happening with your hardware, firmware, software, network connections, and IoT devices. The longer you take to take action the more the problem is insidiously growing in complexity and difficulty. Put a policy in place, implement a control plan, deploy technology asset technology, share the information, and act on it now, and you will lift the curse.

Follow the guidelines provided here and your organization will walk in the light of Technology Asset Management transparency. And in doing so you will avoid the pitfalls of waste, breach, inefficiency, and fear.

nlyte.com