Service dependencies on CIT and A&S IT

We expend time and effort ensuring central services (CIT) and services co-managed by A&S IT end up helping us, and don't actually hurt us.

August 2018: Screen lock "force"

Monday, July 30, 2018 2:41 PM: A&S IT sent a message about a scheduled change for August 8th that they created, and had nothing to do with CIT.

This is the first time a change was going to be forced simply because a computer had software for us to report back its state.

Although this change was consequential, it was going to happen without the usual technical due-diligence to ensure:

1. It did what it was expected to do.
2. It did not do what it was not expected to.

Although this change was consequential, it was going to happen with the usual "governance" and deliberation to ensure:

1. The extent of the problem the change was meant to address.
2. The measure by which the expected change to the systems occurred.

The operational difference between Opt-in and Opt-out

Opting-in requires TSPs to deliberately decide which computers will be acted on using central management tools, if utilized at all to meet operational needs.

Opting-out, with no TSP intervention, uses central management tools to act on every computer.

Examples we've seen so far when opt-in was not sliced-and-diced, and the problems that has caused us

Example: Automatic patching of the OS.

Then Spririon (Identity Finder) added AND had behaviors. Scanning every time a USB device put in. Running scans. These were not appropriate for lecture computers, such as in Physics.

Removing the computer from central patching was extremely non-trivial. Not simply "now opt-out".

Example: Automatic patching of the OS.

Patching for MS OS and MS applications. Also force updates for non-MS, 3rd party applications. Not desirable since we have a superior solution.

The preference for opting-in or opting-out is also driven by convenience and risk management. The more "different" the machines one has, the more critical it is we retain an opt-in infrastructure.

If instead we do opt-out, in research especially we will need to:

Put a computer into every opt-out option group there is.

Category or concern	If opt-in to using specific central management solutions:	If requiring opting-out computers from specific central management solutions:	Real-world examples	Notes
Conflating the capacity to see our systems using central management tools with the obligation to use that same system to by default affect change to those same systems.	This has been the standard of practice, period. Not making changes by default makes it much safer and clearer that the client can afford to be installed. Priority has been to gain visibility of our systems and their configuration. To wit, the university is expending even more efforts to make that visibility more precises and visible within one tool (Remedy Asset Manager).	Requires a high degree of trust in the tools and processes for change. Forced changes are usually not appropriate for some research and classroom systems.		
TSP's role and responsiblity	Deliberately designate systems to be changed. Opportunity and obligation to phase in the use of specific solutions as appropriate to environment. This includes selecting systems, method of verification, over what time-frames. Different solutions will each likely require different verification methodologies, different systems to use first, and timing.			Managers and ITSG can see the degree to which any central management solution is used. And can compare that tool's use with reports on the current state of the computers, bringing attention to bear on non-compliant systems.

Governance and risk	Level of process or testing is proportional to the needs expressed by the TSPs who want to pursuing using a specific solution to solve their challenges.	Deployments have historically been by by decree, with little-to-no process. And very uneven testing. To little consequence of failure for central A&S IT, and high consequence for department IT. Often solutions are sometimes inexplicably linked so opting in or opting out becomes an all-or-nothing proposition. This decreases the potential for TSPs to adopt specific solutions to solve their challenges.		
Technical structure of groups required.	Specific central management solutions are made available by adding computers to specific groups.	All computers by default get specific central management solutions, . Any computer can be opted-out by adding computers to specific groups.		

Oliver's request to A&S IT

We request that software installed on computers to provide connectivity to central computer inventory and management tools **continue** to make no changes by default to any system on which the client is installed.

By giving primacy for clients to report inventory information, and not also by default forcing any changes to a computer, we increase the number of computers which can be characterized using central reporting tools. This importantly increases the number of systems visible within the centrally-provided inventory tool, Remedy Asset Management, all without needing new processes or tools.

Departmental Technical Support Providers (TSP) should direct their efforts to understanding the changes needed by the systems in their area, and opt-in them into using central management solutions is as they see fit.This can happen if management solutions continue to be provided in a slice-and-diced manner. If centrally provided management services are NOT opt-in, TSPs will instead have to make efforts to understand when forced solutions are not appropriate for their systems

not happen to their systems, now and in the future. This will be true even for proposed solution which an area may not have a demonstrated need or desire for. TSPs should not have to be made to make an effort to "defend" ourselves from default actions taken centrally. Instead, every TSP should be responsible to vet any proposed policy they elect to apply to their systems, and subsequently and deliberately put those systems into groups to affect those changes.

I strongly recommend CIT and A&S IT continue making investments to report on the current state of the most critical parameters of our systems with these clients. An important example are the fields being developed with Audit, ITSO, and others within Remedy Asset Management to better characterize our security posture of every single computer which has the client. Of course A&S IT can also invest in developing and vetting solutions to improve on those measures. And when some of those solutions happen to depend on central management clients, do as CIT does and offer them to TSPs so that we may deliberately opt in our systems into the appropriate groups, as best fits the need of each unit.

Additional details

The two management tools used at Cornell are each focused primarily on one of two supported computer operating systems (OS):

- Microsoft's Configuration Management (**CM**), for Microsoft Windows.
  - Chemistry uses CM on xx number of computers, which is yy % of the College's computers using CM.
- Jamf's **Jamf Pro**, for Apple MacOS.
  - Chemistry uses Jamf Pro on xx number of computers, which is yy % of the College's computers using Jamf Pro.

And offer select solutions as opt-in to those who may benefit, on their own schedule.

- Retaining this standard of practice, which has been in place for years (8+ years?) and is enabled by CIT's provisioning of these central services, will increase the number of the college's computer assets in the Chemistry Department made visible to management and audit.
- It's important we continue our efforts to increase the number of our assets made centrally visible, and Increasing the number of assets made visible, concurrent with investments being made to improve reporting within these centralized tools such as putting data into Remedy Asset Management, will also increase the accountability of the configuration these same assets. This can help target our technical and social efforts to further improve our security posture without compromising required functions or trust in centrally-provided tools.
- By compelling IT support providers to opt-in to affecting changes to systems under their management, it will continue to promote a culture of engagement and accountability on when these powerful centralized tools are most effectively brought to bear on identified problems, increasing their effectiveness.

If this long-standing practice were to change, it cannot be done quickly. (8 days, with almost no processing or communication, was recently presumed.) A change will force us in Chemistry to remove the client from many of our systems to better protect ... (flesh out consequences...). Making "forced" changes to computers by default, simply because they are running software to increase their visibility, is neither balanced nor necessary. This is especially true given that these are centrally provisioned tools feeding into central inventory systems, an for which we are not provided viable alternatives.

Language Oliver sent Mike and Fred Fri. 8/10/2018 re: opt-in vs opt-out (in that case, forcing name changes, by default):

To Mike's question, "It would be nice to have a solid reasoning behind why not to enforce the name change on all ARTS computers. What would be the negative effect of this policy in your area?": My continued recommended approach is to spend time working problems of the "collective" highest priority, preferably after getting reports on the current state of the systems. And offer select solutions as opt-in to those who may benefit, on their own schedule.

If such services are NOT opt-in, TSPs will all need to understand exactly what will or will not happen to our systems, now AND in the future, sometimes for a proposed solution which we may not have a need for. TSPs should not have to be made to make an effort to "defend" ourselves from default actions taken centrally. Instead, we each should be responsible to vet any proposed policy we elect to apply to my systems.

So if I may turn your question on its head: It would be nice to have a solid reasoning behind why we must enforce the name change on all ARTS computers. What would be the negative effect of making this policy available to every area?

Additional details

The two management tools used at Cornell are each focused primarily on one of two supported computer operating systems (OS):

- Microsoft's Configuration Management (**CM**), for Microsoft Windows.
    - Chemistry uses CM on xx number of computers, which is yy % of the College's computers using CM.
- Jamf's **Jamf Pro**, for Apple MacOS.
    - Chemistry uses Jamf Pro on xx number of computers, which is yy % of the College's computers using Jamf Pro.

Just having the client installed, even when not doing anything to a computer, provides us (IT professionals, A&S management, and CU Audit) valuable, trustworthy visibility to computers with the clients. Information includes the last time a computer has reported into the central console (implies whether asset is active), the computer's configuration (for example, our screen lock-related settings and if the OS current), software (and their versions) installed.

The client is the ONLY method the university provides and makes investments in to get data automatically into Remedy. Remedy has Cornell-specific fields to help ensure compliance to university policies. Thus we should be promoting the use of these clients. And not do anything to impede their use, such as making changes automatically to systems just because they have the reporting client installed.

CIT provides these tools. CIT, by default, makes no changes to any system on which the client is installed. Arts and Sciences IT should do the same and compel the local IT support providers to "own" changes made to their systems, while facilitating installation of the client on all possible university-owned computer assets.

Chemistry IT has been using these powerful central computer inventory and management tools for many years (8?). Indeed, when we add a Windows computer to AD, we have it automatically install the CM client. Always. Not only do these clients provide central visibility of our computers and their "state", but they also afford us other advantages. These advantages include:

- Enable logging in with NetID.
    - This means our department does not have to manage log-in accounts, such as password resets.
    - Using this technology also provides automatically credentialing to central services such as SFS and policy-based mounting, etc., etc.
- Enable logging in with AD accounts (number of these easy to get? It's many!)
    - Centrally-managed passwords provide for one location to update passwords on many systems at once. distributed among different computer making their management untenable
- Enable easy access via Active Directory.
- Enrolling all our Administrative computers, and many others, to central patching and other "standards" not appropriate to many research systems we also manage.

Of course central computer inventory and management tools can also be used to make changes to computers on which the client is installed.However, these capabilities must be made optional for any given computer and groups make these desired changes easy to apply to many computers at a time.

Oliver's further takes, FWIW

Question

- Was action taken out of ignorance (didn't understand meaning of action, nor it's consequences), irresponsibility (knew potential to harm trust and compromise fidelity of infrastructure but went ahead anyway), or some other reason?

IT professionals should keep some things in mind

Mass-affect technology must be respected.

- Take care what you do for one computer. Take super-deep care what you do for hundreds of computers.

Enable us to use our technology to serve our users by letting us do things for them. Not do things to them.

Enable us to use our technology to better see what we have to see what must change and prioritize areas of concern.

Don't be compelled to use only the tools you have if they don't get you the desired state.

- Be willing to walk away from unacceptable results, regardless of the pressures.

When existing, proven, active technical vetting processes exist, use them or be clear you did not and why.

Just because you can do something doesn't mean you should do something.

- As a corollary, just because a tool appears to do something doesn't mean it does what you hope it will. Especially if you don't ask the right questions when testing it.

Action was presumptive. The change had not followed expected process to reduce chance of technical error and what the change led to the desired outcomes.

Action was arrogant and paternalistic. The change came across as "we know what is good for you and this is good for you; we know better than you. Accept it."

In this case, at least on the Mac side, this approach led to an irresponsible "force". The decision-makers seemed to be disregarding the risks associated with using a powerful tool in a new way which was clearly not technically well understood. ((a configuration change, not a software package deployment)

Oliver's poem inspired by this announcement, August 2, 2018

Watch the do-do

See, before you DO.

Don't DO unless you do due process.

See what you DID.

If you do not do this, you will likely step in DO-DO.

And that stinks for everyone.