Output from Next Gen^2 Network Technical Deep Dive Session - February 12, 2020

Questions discussed: How could the university move in the direction of a zero trust framework and identity-based access? What's needed (people, process, policy, technology)?

Table facilitated by Tom Jordan

People	Process	Policy	Technology
Changing roles/deprovisioning - apps need a way to know	Net IDs don't get de-provisioned - need role information	Explicit decisions/policy needed in order to automate	Campus AD limitations prevent migration - 802.1x and SCEP
Dynamic groups - have some but need more	UDDS is not always a good organizational boundary	Multiple roles/additive privileges/SoD (Segregation of Duties)	More transparent policy engine
Competing priorities - easier to do things locally vs. what's best for the common good	Local department information elevated to use in access control	Polivy vs. authority - reporting lines not always aligned	What formats do we need to present authorization if it is to be useful?
People with multiple roles	Training/education on access management strategy	Policy requires resources to make them real (cost/labor)	
How do we communicate location/device information for users	Approvals need to be timely	Support from deans/department chairs to prioritize security above other things	
Need someone in charge of keeping an eye on the big picture when it comes to integrating apps and infrastructure	Policy for creating accounts on devices	At what level should certain policies be crafted?	
	Identity proofing requirements - social login		

Table facilitated by Pat Christian

People	Process	Policy	Technology
Group is okay with scanning BYODs - May be culture-driven (SMPH may be okay, others not so much) - May encounter "ownership" of devices, whether perceived or actual (e.g. newer vs. older faculty variances)	Clean up RFC1918 space	HR should notify IT when separations occur	Need more virtualization tools to create virtual organizations (schools) distributed on/off campus
	Need deprovisioning process (may get no or limited notice for researchers and staff)	Strip identify of access rights	Need to securely link various credentials to a user identity (Facebook, etc.)
	Need identity and separation of "roles" for researcher/academic (domain model)		Need role-based access
	Network access and who can add/change/delete data		Investment in zero trust can make research more productive (more $$ to UW)
	Frequently fall short on documentation; build template everyone can use		Network needs to use same IAM as apps
	Need "challenge" mechanism if our users + device + location is different/unique		

Table facilitated by Dennis Lange (and Tamra)

People	Process	Policy	Technology
Better understand identity of external users (anonymous)	Faster approval fro a new Manifest group (less than 2 to 3 days)	Enforcement at servers and instruments	Quck access to device and identity status to determine whether to give access
No NetID access (Non-Net ID access?)	Expand use of Manifest - build knowledge! "How to…"	Endpoint security zones	Ability to understand who is in my Manifest group and why
Identity of things (vs. people)	Dynamic off-boarding and transfer process w/department-level hooks.		Better way to represent groups from VPN perspective

Privacy preservation (personal device scans?)			Remove need for people to have a separate NetID on top of other unit ID (e.g. Morgridge, UW Health)
Identify users on the central VPN and use information to enforce department policies			Reduce segmentation of servers by leaning on identity (self-identification)
Developer and sys admin education on network, identity, classifications/security zones			

Table facilitated by Joe Johnson

People	Process	Policy	Technology
HR roles are not meaningful for network access permissions/authorization	Lots of single-person IT shops; what will this change mean for them?	PHI policy drives a lot of design decisions. Will everything expect the same level of rigor, e.g. design for the hardest case?	Things distributed units might want to shed: - Running own email, but PHI is a challenge - Local Sharepoint in favor of a central offering (but multi-institutional nature is hard)
Narrow down the scope - campus too broad, start with an MVP in a single distributed campus unit	Move to campus AD - one year duration (Vet Med). [This was given as an example of a dist. IT unit joining Central IT and the process being slow]	Policies that recognize that schools, colleges, departments, divisions, and institutions are organized differently than one another, and differently than central IT	Zero trust against myriad O/S, lab equipment, etc. Technical disadvantages
UW Health - multiple institutions require IAM and network access, this is challenging	Unit admins are likley to need admin access/flexibility to meet their needs w/single AD, how will that work?		DHCP/DNS self-service that all campus units could consume = need some admin access
Multi-institution centers from outside the UW need IAM and network access	When/how would training occur? We're busy day-to-day.		AANTS - Continue this type of access and enhance/expand to AD and wifi
We have customers that need network access and need to be in IAM that are not employees (CIAM issue)	Endpoints that require older O/S; no patches are available for compliance		Distributed units need access that allows for troubleshooting and monitoring the network layer when things go wrong
	need to develop a broad, reusable methodology to adapt existing workflows to zero trust model		Campus AD doesn't accommodate Linux hosts? [This statement was made, but I don't know that it is accurate]
	Zero trust may help PHI segmentation challenges, could be an inventive to do so		
	How to make zero trust adaptable, appealing, work for the majority?		

Table facilitated by Jeanne Skul

People	Process	Policy	Technology
Extension offices user identity	Provisioning and deprovisioning when employees move	HIPAA	Own credentials in departments
Dual-appointed faculty	Volunteers in 4H, Master Gardener, Extension-managed projects	Lack of policy drove us to current environment	Old technology that can't be updated
Students and student workers	Credential issues - research collaboration with other institutions, other IT deparments, AIMS	Research $$ always win	Asset Inventory Management
Integrated faculty in Extension roles and other universities	Pain of move to one identity (time, resources)		IoT
"Students in resdience" WPM			Classroom media
User name matching			Servers in own forest
Modifying schema SharePoint			