Costs Considerations in Refreshing Vulnerable IT Networks

12 June 2018

John Leahy

Advanced Strategic Enterprise Concepts

Bottom Line Up Front

- IT Networks are vulnerable to Cyber Security intrusions
- Cyber security can be the driving force behind a network refresh and renewal program
- But there are issues -
  - Competing interests among stakeholders
  - Limited funding
  - Availability of labor
- Reconciliation of these issues results in a strategy that falls into two main approaches-
  - Rip and Replace
  - Holistic

Aging Infrastructure is Vulnerable to Data Breaches

- A survey of IT managers in 2017 found that **47 percent** of federal agencies still use **Windows XP**.
- Gartner Group finds legacy systems in the federal government have **an average age of 14 years**, compared to 10 years in the private sector.
- GAO noted reliance on legacy IT can result in **security vulnerabilities** where **old software systems** are **no longer supported** by vendors and **aging IT infrastructure** becomes difficult and expensive to secure.
- PWC said about **80 percent of cyber crime** events result from shortcomings in companies "technology hygiene". In other words, the adversary gained access to a system through **vulnerabilities that were generally known**. Companies' **push to cut spending** has taken a toll on their IT solutions.

Cyber Security Intrusion: The Damage Done

"This is crown jewels material . . . a gold mine for a foreign intelligence service."

"This is not the end of American human intelligence, but it's a significant blow."

- Joel Brenner, former NSA Senior Counsel

"We cannot undo this damage. What is done is done and it will take decades to fix."

- John Schindler, former NSA officer

"[The SF-86] gives you any kind of information that might be a threat to [the employee's] security clearance."

- Jeff Neal, former DHS official

"My SF-86 lists every place I've ever lived since I was 18, every foreign travel I've ever taken, all of my family, their addresses. So it's not just my identity that's affected. I've got siblings. I've got five kids. All of that is in there."

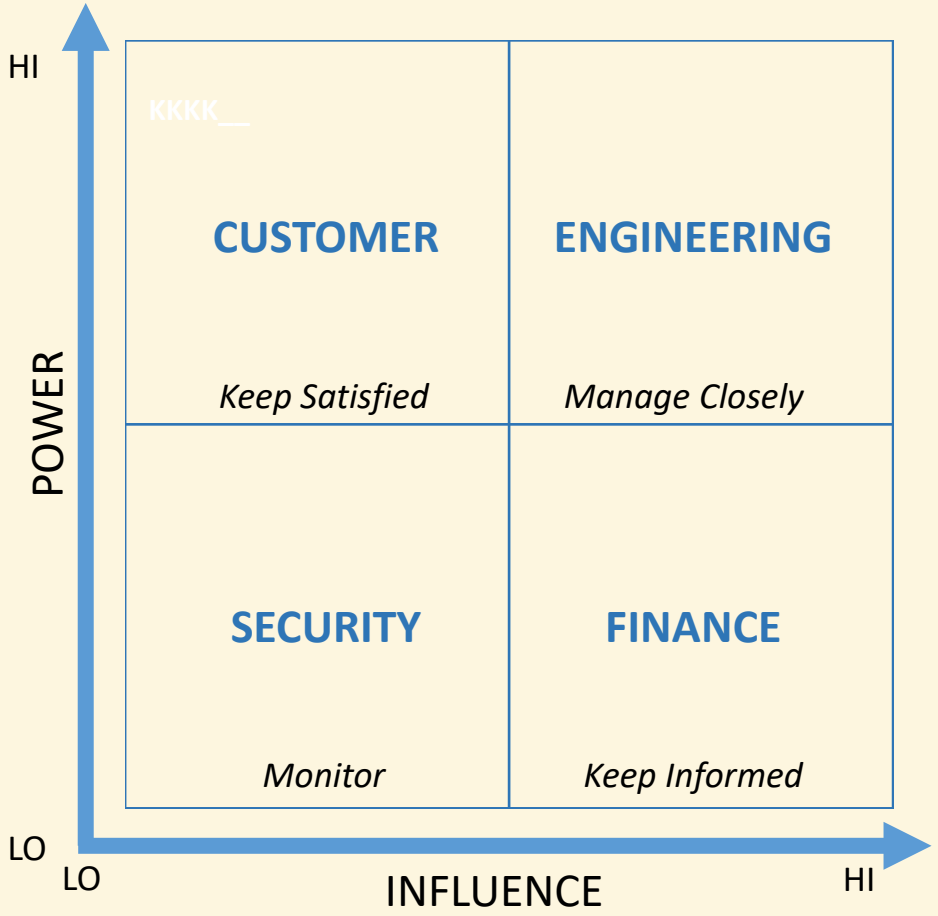
- James Comey, former Director of the FBI

"[OPM data] remains a treasure trove of information that is available to the Chinese until the people represented by the information age off. There's no fixing it"

- Michael Hayden, former Director of the CIA

Committee on Oversight and Government Reform
U.S. House of Representatives 114th Congress
The OPM Breach: How the Government Jeopardized Our National Security for More than a Generation

IT Network Stakeholders – Approach Strategy



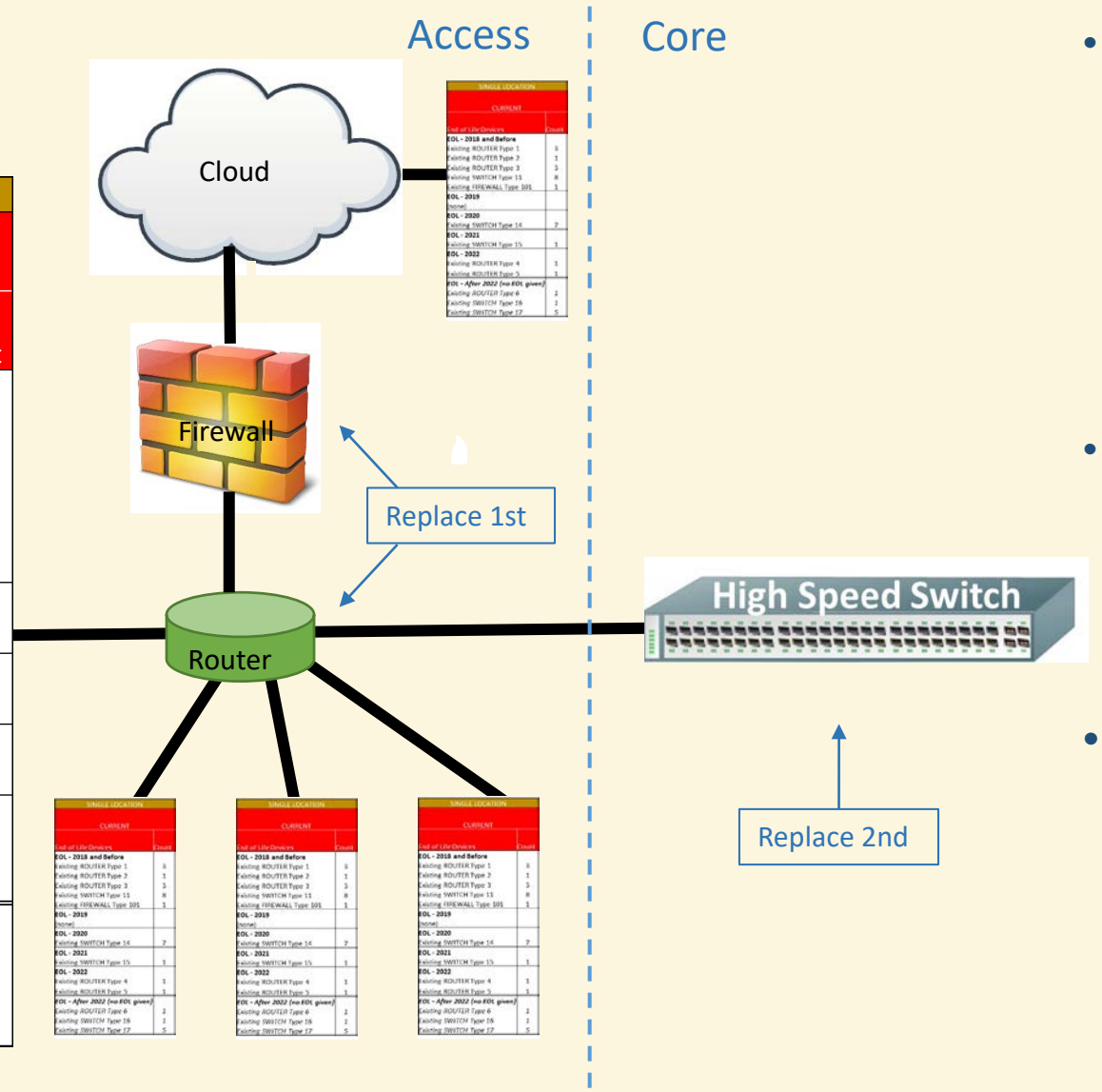
- In addressing security within an IT network key stakeholders must be identified
- These stakeholders can be impacted by the project – either positively or negatively
- They have varying degrees of power and influence over the project

IT Network Stakeholders

	Key Requirements	Power and Influence
Customers	- Network infrastructure up and running - Increase capacity and availability to handle escalating mission needs	- Direct path to senior leadership - Influence corporate direction
Engineering	-Improve network service agility and interoperability through consolidation - Combine disparate systems into a single enterprise network - Integrate functions and capabilities to flatten equipment hierarchy	- Responsible for designing and upgrading network - Approves additions to network
Security	- Refresh vulnerable non-supported and obsolete equipment	- Certifies which devices may operate as part of network
Finance	- Move toward new technologies that reduce capital and operational expense	- Determines pace of network funding for renewal and expansion - Controls funding

IT Network Devices

SINGLE LOCATION	
CURRENT	
End of Life Devices	Count
EOL - 2018 and Before	
Existing ROUTER Type 1	3
Existing ROUTER Type 2	1
Existing ROUTER Type 3	3
Existing SWITCH Type 11	8
Existing FIREWALL Type 101	1
EOL - 2019	
(none)	
EOL - 2020	
Existing SWITCH Type 14	7
EOL - 2021	
Existing SWITCH Type 15	1
EOL - 2022	
Existing ROUTER Type 4	1
Existing ROUTER Type 5	1
EOL - After 2022 (no EOL given)	
Existing ROUTER Type 6	*1*
Existing SWITCH Type 16	*1*
Existing SWITCH Type 17	*5*



- Each location comprises both Access and Distribution nodes
  - Assume same mix of equipment at each location in the network – in this case, assume 5 locations
  - In reality, varying device combinations at each location results in more options for addressing security vulnerabilities
- Over 40% of Devices are at End of Life
  - Not atypical – suggests equipment refresh has been deferred over the years
  - Devices with no EOL date eventually must also be refreshed
- Position of Stakeholders

Stakeholder	Reaction
Security	Alarm
Finance	More Cost
Engineering	Opportunity
Customer	Indifference

Network Technical Strategy

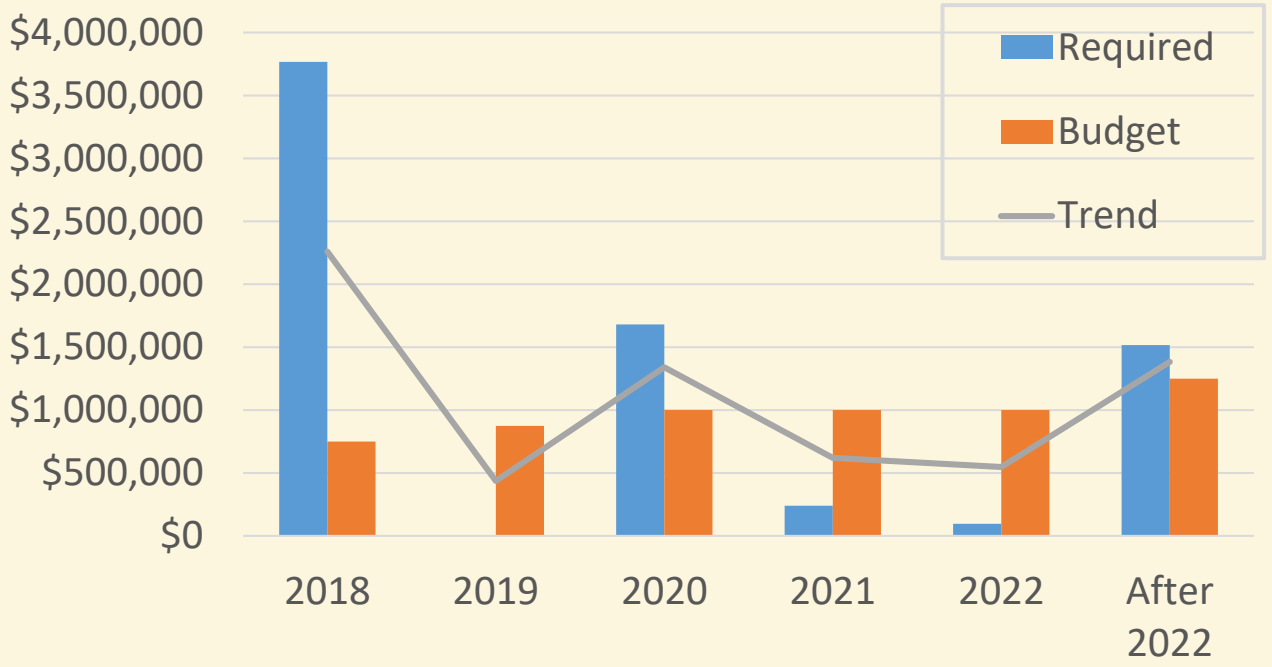
Rip and Replace – Vendor-centric

- With this classic approach the old model is replaced with the vendor recommended new model
  - Vendors are unaware of what other devices a network may contain
  - Focus is on maintaining interoperability characteristics found on older model
- Vendor strategy typically is to offer devices that support their overarching strategy
  - Lock customers in for vendor products
  - A growing tendency to move to software defined networks
  - Vendor's software licensing costs are substituted for internal O&M workforce

Holistic – Enterprise-centric

- Internal engineering upgrades network on a location by location basis
- Requires a solid customer developed network strategy
- Multiple vendors used presenting more options for Engineering
  - For instance, consider using software for access and distribution, but electricity in the core

5 Year Requirement vs Budget



- Only minimal network replacement has been done
  - 40% EOL by value in 2018
- Even if funding were available in 2018 as a one time supplement . . .
  . . . it is unlikely there would be sufficient labor to execute the program

Rip and Replace Refresh Plan

SINGLE LOCATION		ALL 5 LOCATIONS												
CURRENT		VENDOR RECOMMENDED												
End of Life Devices	Count	EOL Count	Replacement Device	Unit Cost	ROUTER Series 51	SWITCH Type 16	FIREWALL Series 601	SWITCH Series 64	SWITCH Series 65	ROUTER Type 6	SWITCH Type 17	Budget	Spend Plan
EOL - 2018 and Before												**$750,000**	**$745,000**
Existing ROUTER Type 1	3												
Existing ROUTER Type 2	1	**35**	**New ROUTER Series 51**	$6,500	35								
Existing ROUTER Type 3	3												
Existing SWITCH Type 11	8 →	**40**	Existing SWITCH Type 16	$70,000		5							
Existing FIREWALL Type 101	1 →	**5**	**New FIREWALL Series 601**	$33,500			5						
EOL - 2019												**$875,000**	**$870,000**
(none)						12		1					
EOL - 2020												**$1,000,000**	**$980,000**
Existing SWITCH Type 14	7 →	**35**	**New SWITCH Series 64**	$30,000		11		7					
EOL - 2021												**$1,000,000**	**$999,500**
Existing SWITCH Type 15	1 →	**5**	**New SWITCH Series 65**	$55,000	3	7		9	4				
EOL - 2022												**$1,000,000**	**$990,500**
Existing ROUTER Type 4	1	**10**	**New ROUTER Series 51**	$6,500	7	5		18	1				
Existing ROUTER Type 5	1												
EOL - After 2022 (no EOL given)												*$1,250,000*	*TBD*
Existing ROUTER Type 6	*1 →*	**5**	*Existing ROUTER Type 6*	*$120,000*									
Existing SWITCH Type 16	*1 →*	**5**	*Existing SWITCH Type 16*	*$70,000*									
Existing SWITCH Type 17	*5 →*	**25**	*Existing SWITCH Type 17*	*$48,000*									
					45	**40**	**5**	**35**	**5**			**$4,625,000**	**$4,585,000**

Rip and Replace

- Assumptions
  - Spend Plan cannot exceed Budget
  - Labor constrained; difficult to increase headcount
  - All 5 locations have same configuration
- With Rip and Replace the older model is replaced with the newer model across all locations
- Some devices (e.g. SWITCH Type 16, , SWITCH Series 64, SWITCH Series 64) need to be deployed immediately,
  - Funding and labor scarcity . . . . . dictate the upgrade must be accomplished over several years
- Although some devices have not reached EOL, they must be considered in any plan

Rip and Replace Plan Stakeholder Perspectives

	Rip and Replace
Customers	PRO – Viewed as improvements to network to keep it up and running
	CON – Belief that any network improvements may not be worth the disruptions
Engineering	PRO – Predictable method of insuring vendor supported device
	CON – Puts off interoperability through consolidation
Security	PRO – EOL devices replaced sooner making them compliant
	CON – May be multiple devices requiring security approval slowing down implementation
Finance	PRO – Smaller projects make it easier to move forward with refresh in the face of uncertain funding
	CON – Retards movement toward technologies that reduce capital and operational expense

Budget mismatch with Requirements results in replacements being deferred until later years when Budget, Requirements more in synch

Holistic Refresh Plan

SINGLE LOCATION		ALL 5 LOCATION							
CURRENT		PREFERRED			SWITCH/ROUTER Model 91	FIREWALL Series 601	SWITCH/ROUTER Model 92		
End of Life Devices	Count	Count	Replacement Device	Unit Cost				Budget	Spend Plan
EOL - 2018 and Before								**$750,000**	**$743,500**
Existing ROUTER Type 1	3	0	SWITCH/ROUTER Model 91	$48,000					
Existing ROUTER Type 2	1	0	SWITCH/ROUTER Model 91	$48,000					
Existing ROUTER Type 3	3	0	SWITCH/ROUTER Model 91	$48,000					
Existing SWITCH Type 11	8 →	40	SWITCH/ROUTER Model 91	$48,000	12				
Existing FIREWALL Type 101	1 →	5	New FIREWALL Series 601	$33,500		5			
EOL - 2019								**$875,000**	**$864,000**
(none)					18				
EOL - 2020								**$1,000,000**	**$960,000**
Existing SWITCH Type 14	7 →	35	SWITCH/ROUTER Model 91	$48,000	20				
EOL - 2021								**$1,000,000**	**$960,000**
Existing SWITCH Type 15	1 →	5	SWITCH/ROUTER Model 91	$48,000	20				
EOL - 2022								**$1,000,000**	**$480,000**
Existing ROUTER Type 4	1	0	SWITCH/ROUTER Model 91		10				
Existing ROUTER Type 5	1	0	SWITCH/ROUTER Model 91						
EOL - After 2022 (no EOL given)								*$1,250,000*	*TBD*
Existing ROUTER Type 6	*1 →*	*0*	*SWITCH/ROUTER Model 91*	*$48,000*					
Existing SWITCH Type 16	*1 →*	*5*	*SWITCH/ROUTER Model 91*	*$48,000*					
Existing SWITCH Type 17	*5 →*	*25*	*SWITCH/ROUTER Model 92*	*$60,000*					
					80	**5**		**$4,625,000**	**$4,007,500**

Holistic

- Assumptions
  - Same as before
- With a Holistic approach a comprehensive solution is chosen for each of the locations
  - In this case, the SWITCH/ROUTER Model 91
- Refresh was deferred for several years
  - Even though the solution is well suited for the location . . .
    . . . it will take several years before it is fully implemented
- The holistic approach results in cost savings
  - This can be applied toward refreshing the Core infrastructure in the out years

Holistic Plan and Stakeholder Perspectives

	Holistic
Customers	PRO – Provides more capabilities
	CON – Some locations may lag behind others by several years before realizing major improvements
Engineering	PRO – Improve network service agility and combine disparate systems into a single enterprise network
	CON –Smaller, but important network projects subservient to master plan at each location
Security	PRO – Fewer devices with longer lives simplifies security approval
	CON – EOL devices replaced much later in cycle increasing cybersecurity vulnerability
Finance	PRO – Efficiencies increase as integrated functions and capabilities flatten equipment hierarchy
	CON – Some EOL devices may require replacement in the near term, but become redundant by a more comprehensive solution later

Holistic plan offers sufficient cost savings over rip and replace
that some core infrastructure can be replaced in the out years

Take Aways

- Frequently, the refresh plan will be dictated by how budgets are constructed
  - A bow wave of delayed refresh creates a significant funding requirement in the early years
  - However, labor may not be readily available to implement the project even if funding is available
  - A refresh cycle may need to fit these constraints
- Stakeholder management is crucial to the viability of the refresh program
  - Understand and address the often conflicting goals/objectives of stakeholders
  - Any one stakeholder can derail the project
- Compromises must be made between ideal engineering solution vs. immediate results
  - Concrete results necessary in the short term for continued program support
  - Seek an equilibrium between an elegance and adequacy in a technical solution
  - A new network architecture can unfold over time
- Network security is a continuous process
  - The notion of having all device compliant is unlikely
  - Instead understand the security risks and choose an appropriate mitigation strategy
- Provide customers with a broad, but limited, IT network
  - It is not practical to provide a solution to all requirements
  - Consider transferring the cost burden of specialized network, including maintenance, back to the customer

IT's a Balancing Act

- Given funding that maybe limited and not match up with requirements . . .
- Decide what security risks are acceptable . . .
- To gain sufficient time to implement a new architecture . . .
- While ensuring customers experience no degradation in service levels

QUESTIONS?