Stand alone Not-for-Profit Community Hospital

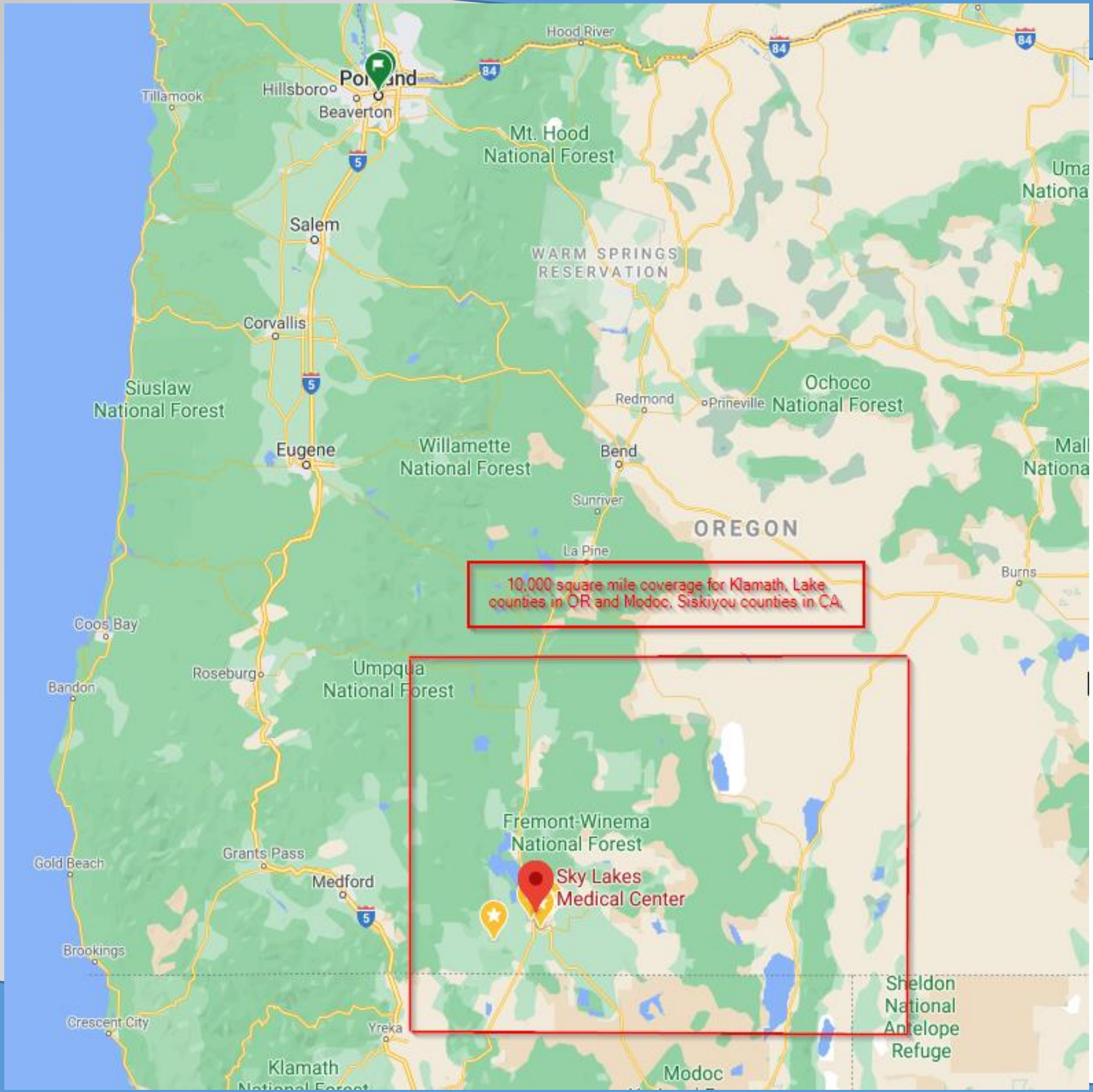
Sky Lakes Medical Center – Overview Stats

- Number of employees: Appx 1,550 FTE + almost 300 Volunteers
- Catchment area:
  - Klamath and Lake counties, Oregon,
  - Modoc and Siskiyou counties, California.
- Amounts to appx 10,000 square miles.
- Outpatient visits: >400,000 a year

Sky Lakes Medical Center – Overview Stats

- Emergency Dept. visits: appx 28,000 a year
- Inpatient discharges: >5,100 a year
- Gross patient revenue: >$550 million a year

Rural Medicine . . .



10,000 square mile coverage for Klamath, Lake counties in OR and Modoc, Siskiyou counties in CA

Stand alone Not-for-Profit Community Hospital

138 Miles North to St. Charles Health System – Bend Oregon

ford Children's Clinic
Sky Lakes Medical Center
Sky Lakes Medical Center
Campus Dr
Daggett Ave
Daggett Ave
Sky Lakes Primary
Sky Lakes Women's Health Clinic
Bryant Williams Dr
Andrew J. Smith, DMD Klamath Falls Dentist
Dermatology Clinic
Mountain View Blvd
Children's Clinic of Klamath
Klamath Falls Foot and Ankle, LLC: Dr. Jeff...
Clairmont Dr
Clairmont Dr
Clairmont Dr

72 Miles West to Asante Health System – Medford Oregon

98 Miles East to Lake District Hospital – Lakeview Oregon

99 Miles South to Modoc Medical Center (Critical Access Hospital) – Alturas California

Ryuk Ransomware Event Monday 10/26/2020

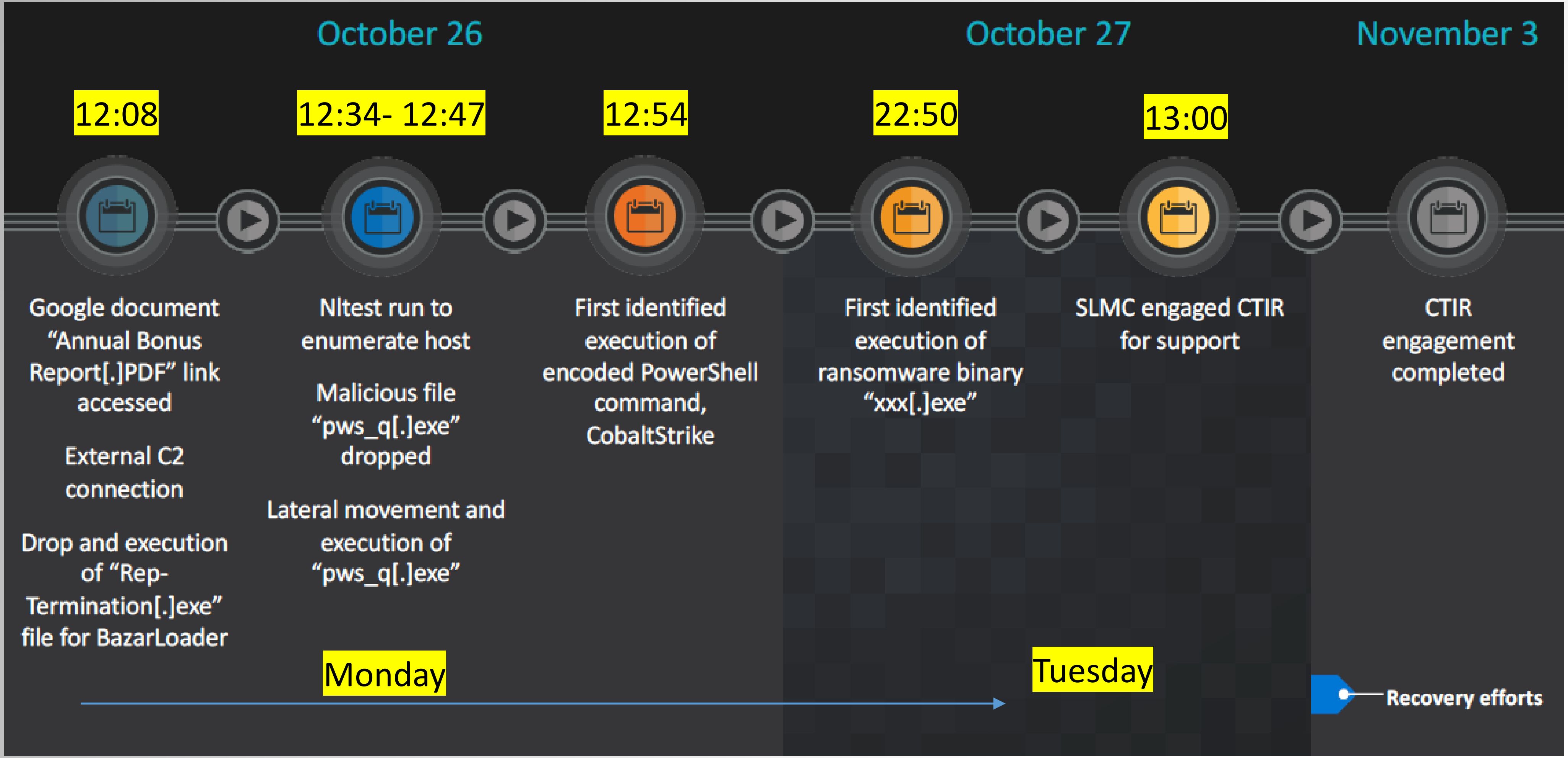
Imagine the 03:30 am phone call . . . ‘we have been hit with ransomware’

The First Call /Symptom . . .

At approximately 0130 PST on Tuesday October 27th Information Services received a call from an end user complaining about system slowness. The on-call person began researching a performance issue – "system slowness."

What happened?

Talos – Incident Response Timeline



October 26

12:08

Google document "Annual Bonus Report[.]PDF" link accessed

External C2 connection

Drop and execution of "Rep-Termination[.]exe" file for BazarLoader

12:34- 12:47

Nltest run to enumerate host

Malicious file "pws_q[.]exe" dropped

Lateral movement and execution of "pws_q[.]exe"

12:54

First identified execution of encoded PowerShell command, CobaltStrike

October 27

22:50

First identified execution of ransomware binary "xxx[.]exe"

13:00

SLMC engaged CTIR for support

November 3

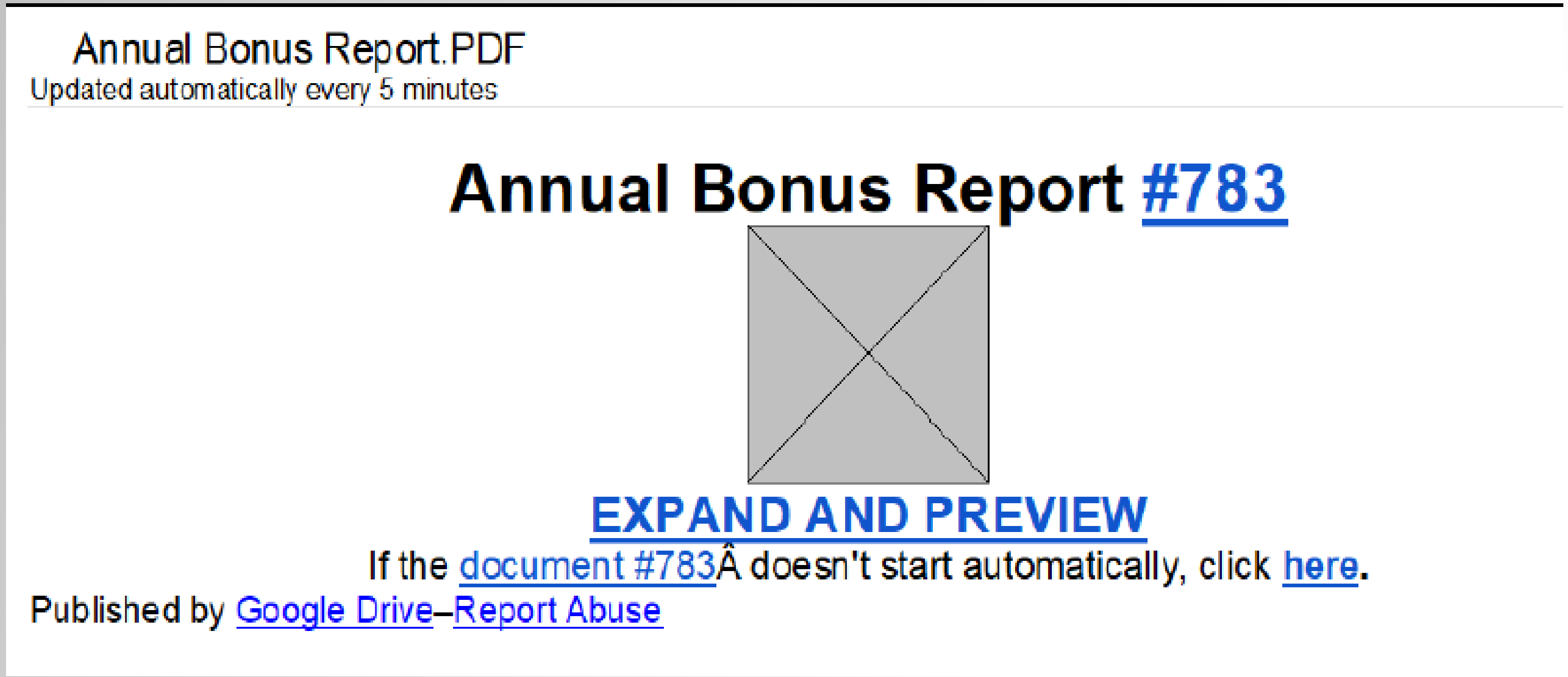
CTIR engagement completed

Monday

Tuesday

Recovery efforts

The Attack Vector . . .



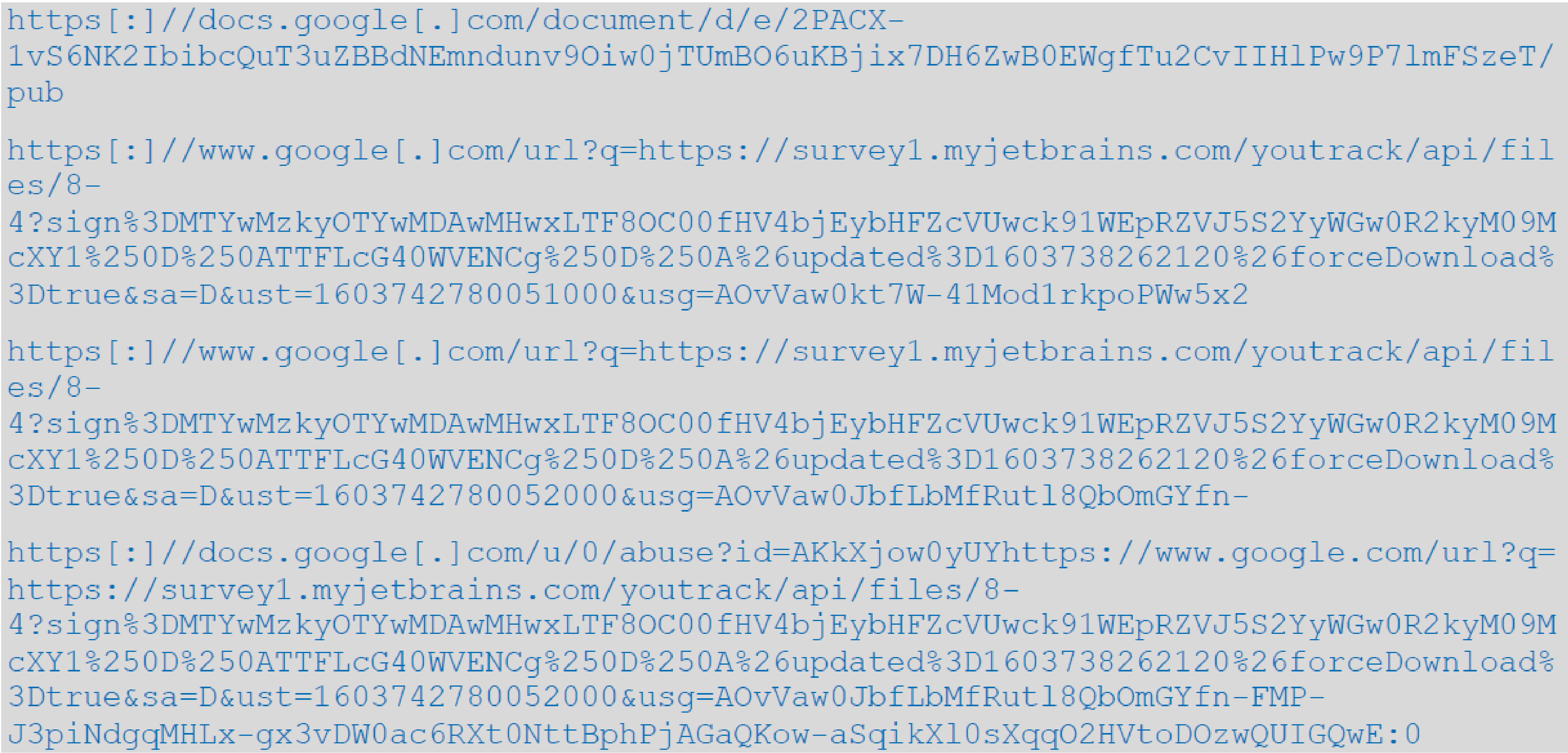
Annual Bonus Report.PDF
Updated automatically every 5 minutes

Annual Bonus Report #783

EXPAND AND PREVIEW
If the document #783Â doesn't start automatically, click here.
Published by Google Drive–Report Abuse

At 12:08 PST on Monday October 26th an employee of Sky Lakes Medical Center (SLMC) clicked on a google document link from an email that offered a "bonus."

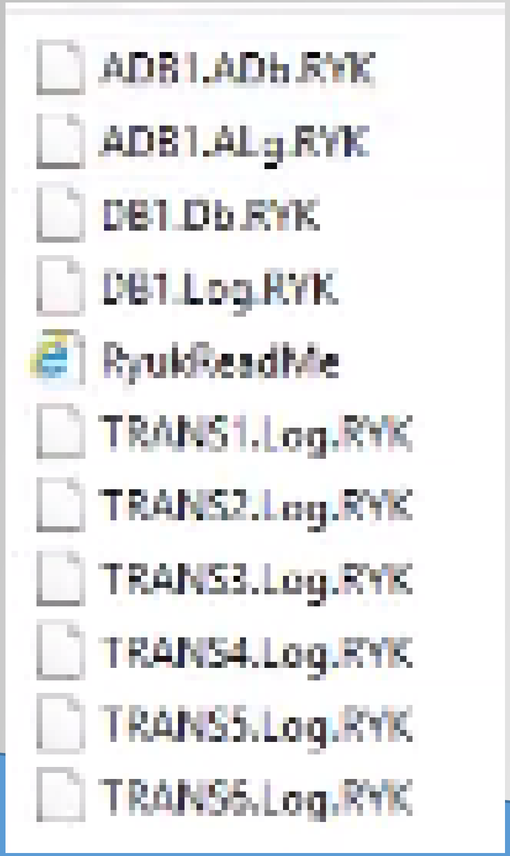
The Attack Vector . . .



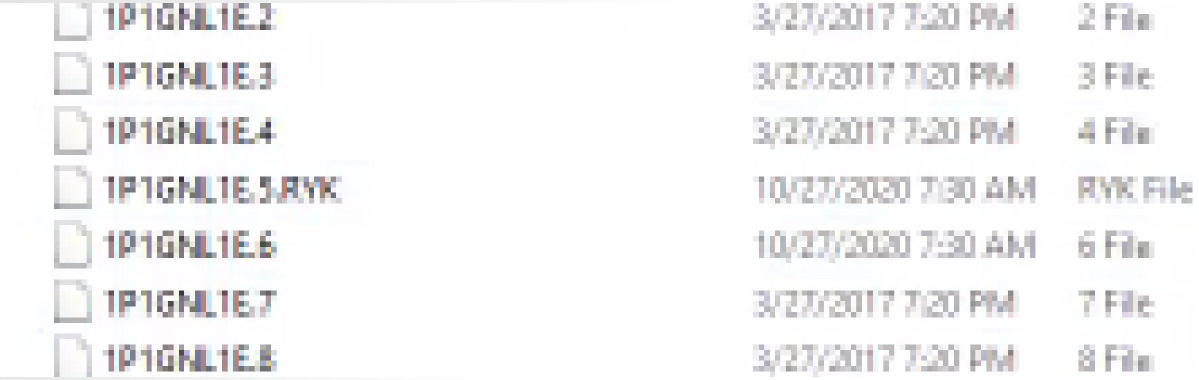
```
https[:]//docs.google[.]com/document/d/e/2PACX-1vS6NK2IbibcQuT3uZBBdNEmndunv9Oiw0jTUmBO6uKBjix7DH6ZwB0EWgfTu2CvIIHlPw9P7lmFSzeT/pub

https[:]//www.google[.]com/url?q=https://survey1.myjetbrains.com/youtrack/api/files/8-4?sign%3DMTYwMzkyOTYwMDAwMHwxLTF8OC00fHV4bjEybHFZcVUwck91WEpRZVJ5S2YyWGw0R2kyM09McXY1%250D%250ATTFLcG40WVENCg%250D%250A%26updated%3D1603738262120%26forceDownload%3Dtrue&sa=D&ust=1603742780051000&usg=AOvVaw0kt7W-41Mod1rkpoPWw5x2

https[:]//www.google[.]com/url?q=https://survey1.myjetbrains.com/youtrack/api/files/8-4?sign%3DMTYwMzkyOTYwMDAwMHwxLTF8OC00fHV4bjEybHFZcVUwck91WEpRZVJ5S2YyWGw0R2kyM09McXY1%250D%250ATTFLcG40WVENCg%250D%250A%26updated%3D1603738262120%26forceDownload%3Dtrue&sa=D&ust=1603742780052000&usg=AOvVaw0JbfLbMfRutl8QbOmGYfn-

https[:]//docs.google[.]com/u/0/abuse?id=AKkXjow0yUYhttps://www.google.com/url?q=https://survey1.myjetbrains.com/youtrack/api/files/8-4?sign%3DMTYwMzkyOTYwMDAwMHwxLTF8OC00fHV4bjEybHFZcVUwck91WEpRZVJ5S2YyWGw0R2kyM09McXY1%250D%250ATTFLcG40WVENCg%250D%250A%26updated%3D1603738262120%26forceDownload%3Dtrue&sa=D&ust=1603742780052000&usg=AOvVaw0JbfLbMfRutl8QbOmGYfn-FMP-J3piNdgqMHLx-gx3vDW0ac6RXt0NttBphPjAGaQKow-aSqikXl0sXqqO2HVtoDOzwQUIGQwE:0
```

The actual Google Docs link to the Zero Day malicious site

Encrypted Imaging Files

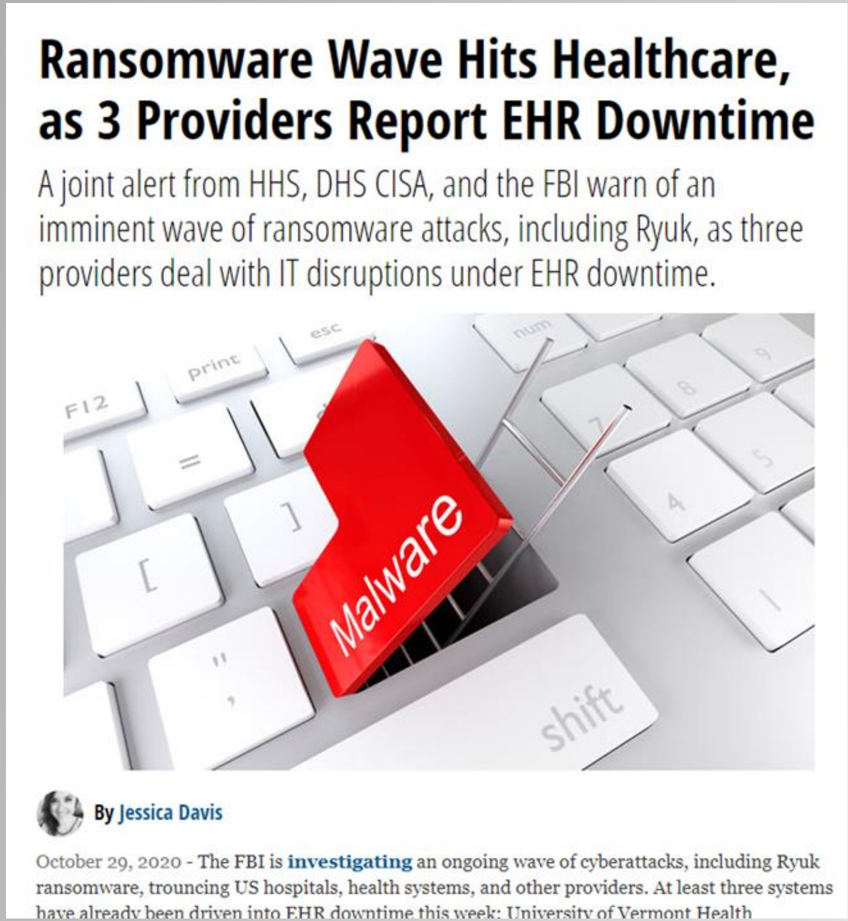


```
ADB1.ADb.RYK
ADB1.ALg.RYK
DB1.Db.RYK
DB1.Log.RYK
RyukReadMe
TRANS1.Log.RYK
TRANS2.Log.RYK
TRANS3.Log.RYK
TRANS4.Log.RYK
TRANS5.Log.RYK
TRANS6.Log.RYK
```



```
1P1GNL1E.2          3/27/2017 7:20 PM     2 File
1P1GNL1E.3          3/27/2017 7:20 PM     3 File
1P1GNL1E.4          3/27/2017 7:20 PM     4 File
1P1GNL1E.5.RYK      10/27/2020 7:30 AM    RYK File
1P1GNL1E.6          10/27/2020 7:30 AM    6 File
1P1GNL1E.7          3/27/2017 7:20 PM     7 File
1P1GNL1E.8          3/27/2017 7:20 PM     8 File
```

Cybercrime – Warning . . .



Ransomware Wave Hits Healthcare, as 3 Providers Report EHR Downtime

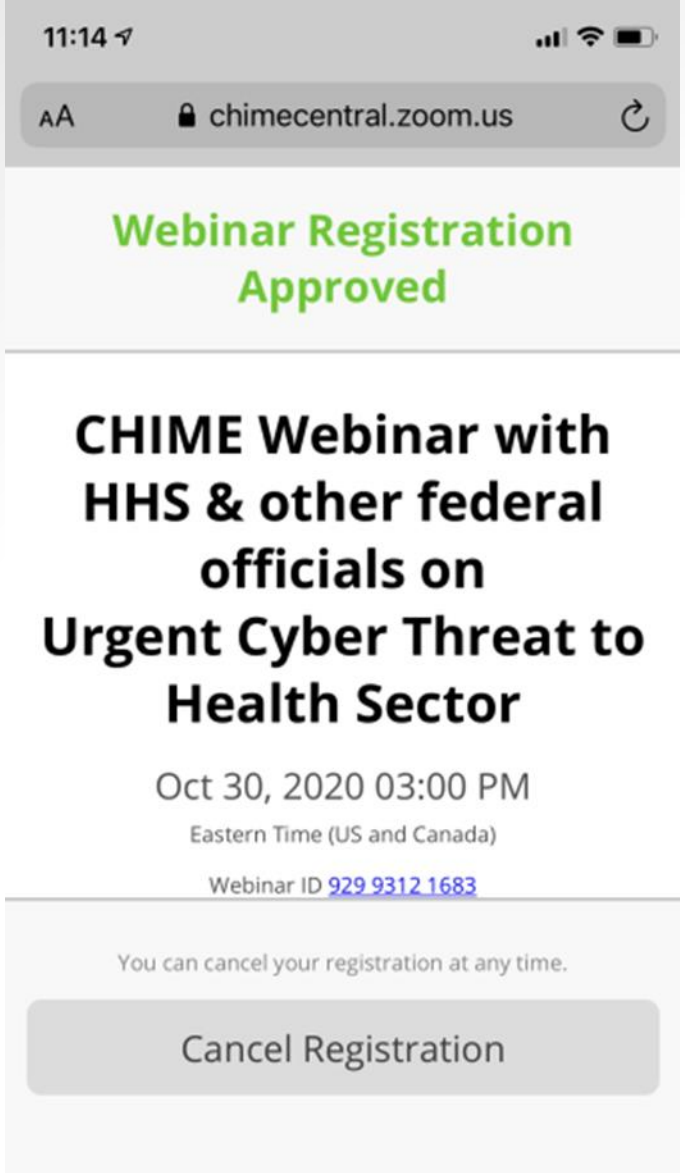
A joint alert from HHS, DHS CISA, and the FBI warn of an imminent wave of ransomware attacks, including Ryuk, as three providers deal with IT disruptions under EHR downtime.

Malware
shift
print
esc
F12
num

By Jessica Davis

October 29, 2020 - The FBI is **investigating** an ongoing wave of cyberattacks, including Ryuk ransomware, trouncing US hospitals, health systems, and other providers. At least three systems have already been driven into EHR downtime this week: University of Vermont Health

The Federal Bureau of Investigation, Department of Homeland Security and Department of Health and Human Services warned hospitals in October of an "increased and imminent" threat from hackers.



11:14

AA chimecentral.zoom.us

Webinar Registration Approved

CHIME Webinar with HHS & other federal officials on Urgent Cyber Threat to Health Sector

Oct 30, 2020 03:00 PM

Eastern Time (US and Canada)

Webinar ID 929 9312 1683

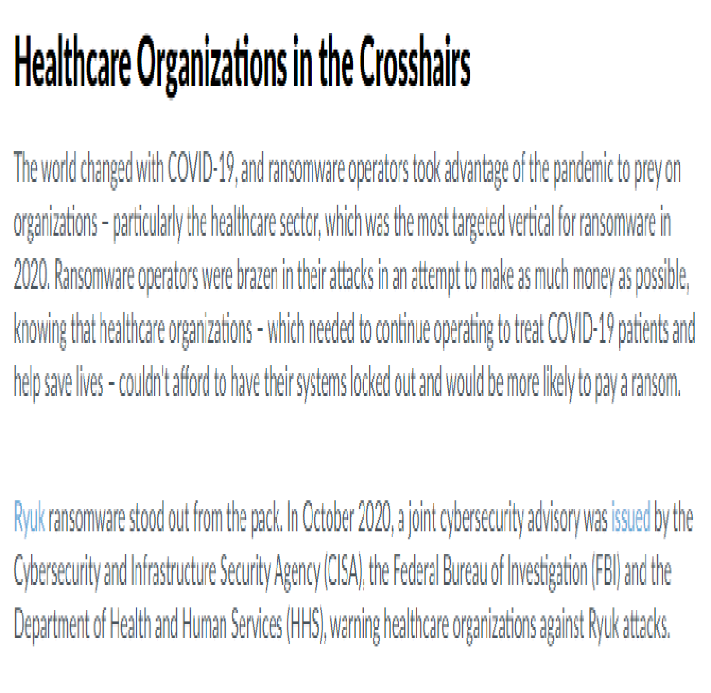
You can cancel your registration at any time.

Cancel Registration

WSJ, *Cyberattacks Cost Hospitals Millions During Covid*, Melanie Evans and Robert McMillian, accessed 02/26/2021

https://healthitsecurity.com/news/ransomware-wave-hits-healthcare-as-3-providers-report-ehr-downtime

Cybercrime – Healthcare a prime target . . .



Healthcare Organizations in the Crosshairs

The world changed with COVID-19, and ransomware operators took advantage of the pandemic to prey on organizations - particularly the healthcare sector, which was the most targeted vertical for ransomware in 2020. Ransomware operators were brazen in their attacks in an attempt to make as much money as possible, knowing that healthcare organizations - which needed to continue operating to treat COVID-19 patients and help save lives - couldn't afford to have their systems locked out and would be more likely to pay a ransom.

Ryuk ransomware stood out from the pack. In October 2020, a joint cybersecurity advisory was issued by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI) and the Department of Health and Human Services (HHS), warning healthcare organizations against Ryuk attacks.

Healthcare Organizations in the Crosshairs
The world changed with COVID-19, and ransomware operators took advantage of the pandemic to prey on organizations – particularly the healthcare sector, **which was the most targeted vertical for ransomware in 2020**. Ransomware operators were brazen in their attacks in an attempt to make as much money as possible, knowing that healthcare organizations – which needed to continue operating to treat COVID-19 patients and help save lives – couldn't afford to have their systems locked out and would be more likely to pay a ransom.

Highlights from the 2021 Unit 42 Ransomware Threat Report (paloaltonetworks.com) accessed 03/19/2021

Initial Challenges – The Perfect Storm . . .

- Current TAC case on our hyper-converged infrastructure (HCI) server platform (delayed troubleshooting)
- Cisco AMP for Endpoints was not yet fully deployed (about a month into the new deployment)
- Cisco AMP for Endpoints was not yet fully configured for blocking the execution of malware

Initial Challenges - Working with Cyber Insurance

Talos

1. Attempt to determine root cause
2. Provide expert guidance on recovery

Kivu

1. Recover offline systems
2. Compare Talos findings and any other cross contamination of systems

https://kivuconsulting.com/

Next Steps . . . First Steps

A

1) Strategy – Segment the Network - Shut all systems off – all systems offline.
   A. Protect against further infections
   B. Decrease lateral movement
   C. Shut systems off enterprise wide

SKY LAKES MEDICAL CENTER
LIFE : HEALING : PEACE

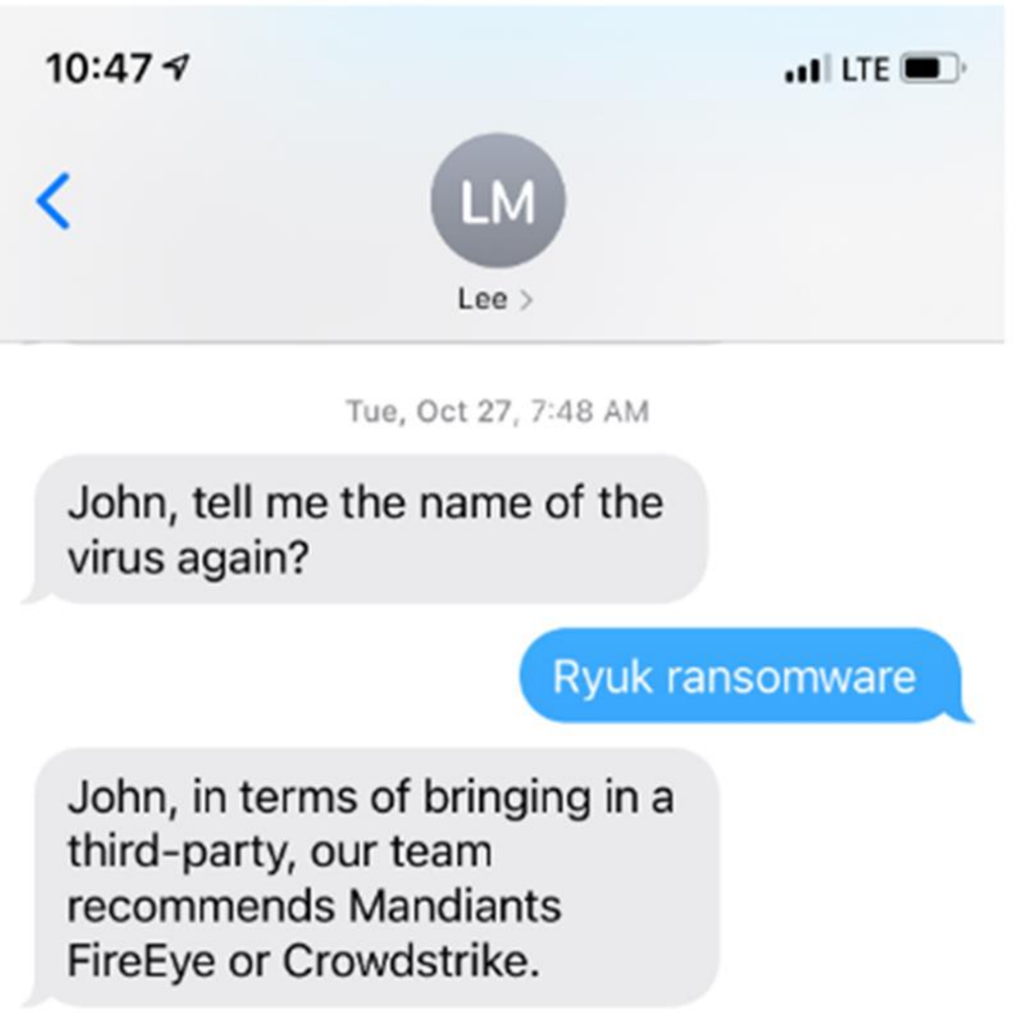
Next Steps . . . First Steps

B

Contact Asante Health System (AHS) leadership to disconnect systems from SLMC

A. Connections - Tunnels
B. Citrix
C. Access
D. Systems

- Asante – CIO notified about at 07:27 am.



Tue, Oct 27, 7:48 AM

John, tell me the name of the virus again?

Ryuk ransomware

John, in terms of bringing in a third-party, our team recommends Mandiants FireEye or Crowdstrike.

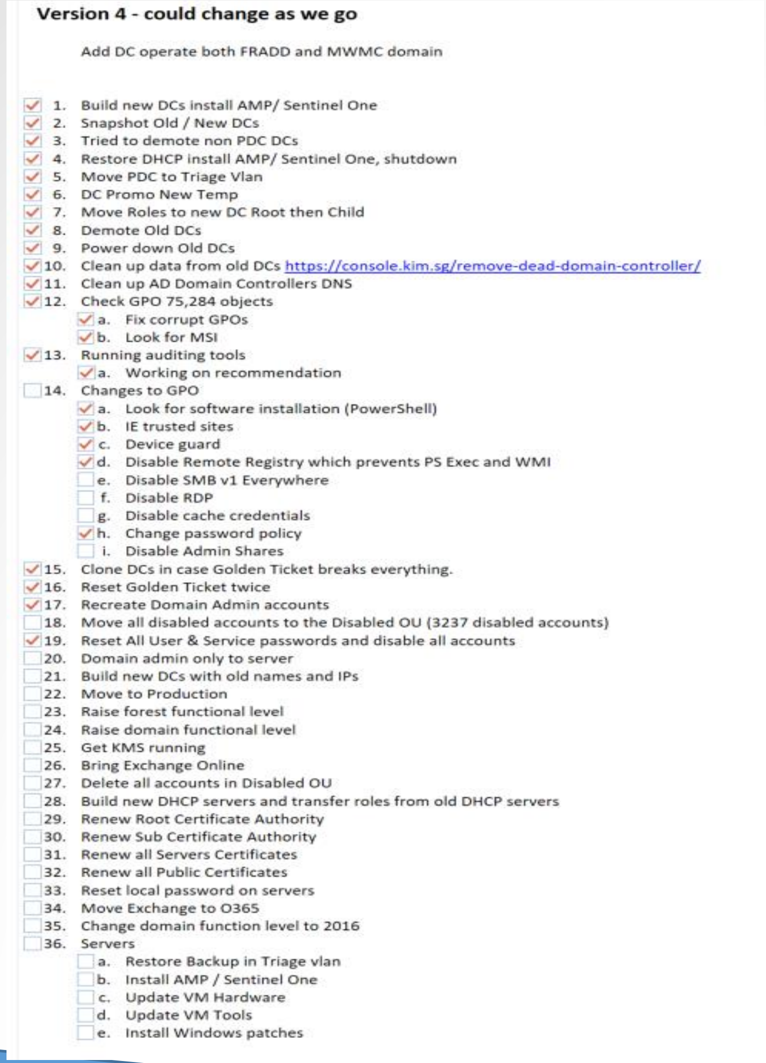
Next Steps . . . First Steps

C

1) Establish a command center – 2nd floor – General Education Conference Room as well as Seven Lakes meeting room
2) Establish communications – daily huddles – 0815 Huddle and 1700 Huddle – hospital wide
3) Commination limited to Cisco WebEx (Teams) which had been established due to COVID-19 back in February 2020.

Next Steps . . . First Steps D

- Many versions of prioritization of Severs
  - Example of upcoming snowstorm and the ability to have facility services run their heating systems for external surfaces

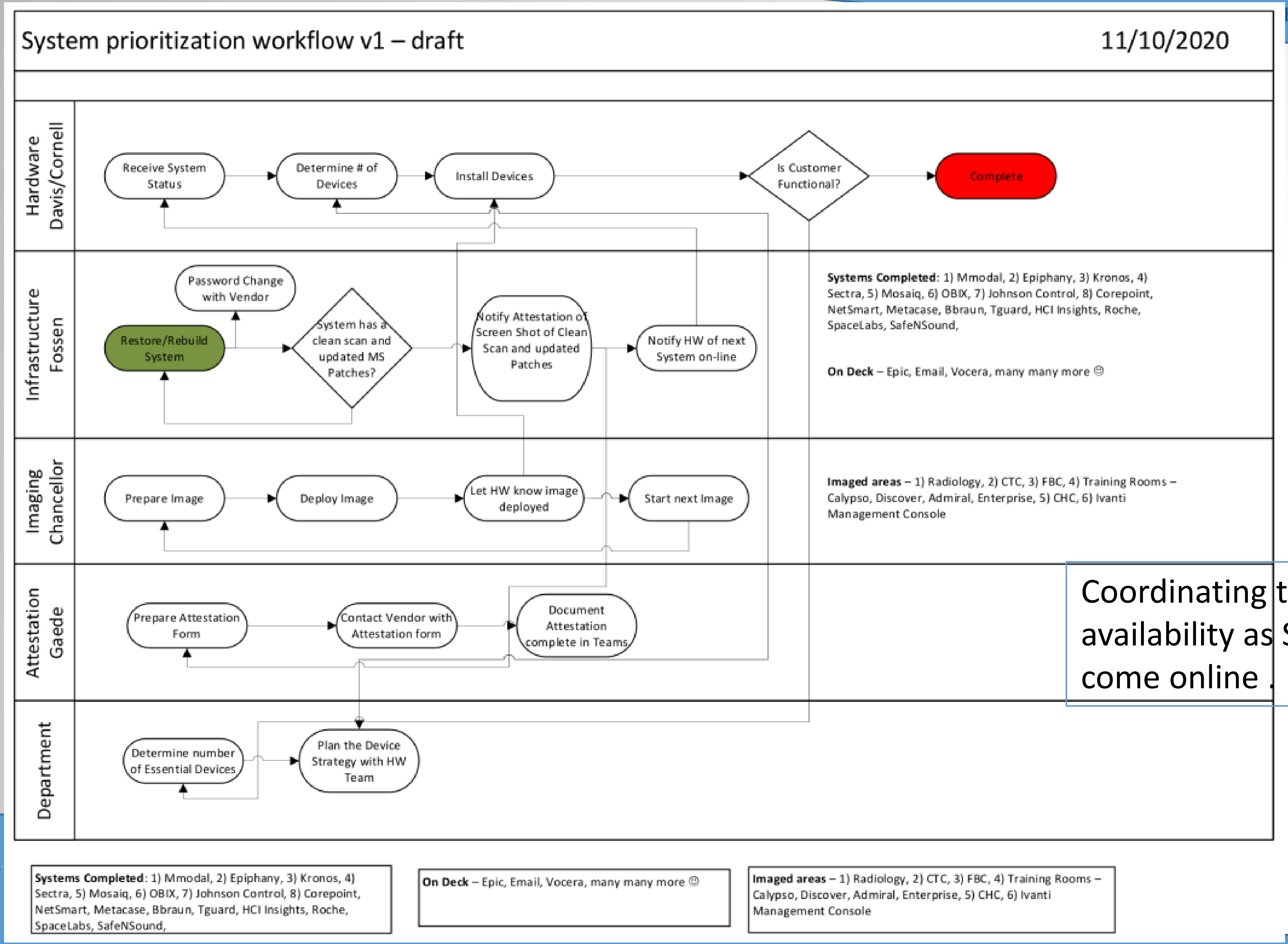


Version 4 - could change as we go

Add DC operate both FRADD and MWMC domain

☑ 1. Build new DCs install AMP/ Sentinel One
☑ 2. Snapshot Old / New DCs
☑ 3. Tried to demote non PDC DCs
☑ 4. Restore DHCP install AMP/ Sentinel One, shutdown
☑ 5. Move PDC to Triage Vlan
☑ 6. DC Promo New Temp
☑ 7. Move Roles to new DC Root then Child
☑ 8. Demote Old DCs
☑ 9. Power down Old DCs
☑ 10. Clean up data from old DCs https://console.kim.sg/remove-dead-domain-controller/
☑ 11. Clean up AD Domain Controllers DNS
☑ 12. Check GPO 75,284 objects
  ☑ a. Fix corrupt GPOs
  ☑ b. Look for MSI
☑ 13. Running auditing tools
  ☑ a. Working on recommendation
□ 14. Changes to GPO
  ☑ a. Look for software installation (PowerShell)
  ☑ b. IE trusted sites
  ☑ c. Device guard
  ☑ d. Disable Remote Registry which prevents PS Exec and WMI
  □ e. Disable SMB v1 Everywhere
  □ f. Disable RDP
  □ g. Disable cache credentials
  ☑ h. Change password policy
  □ i. Disable Admin Shares
☑ 15. Clone DCs in case Golden Ticket breaks everything.
☑ 16. Reset Golden Ticket twice
☑ 17. Recreate Domain Admin accounts
□ 18. Move all disabled accounts to the Disabled OU (3237 disabled accounts)
☑ 19. Reset All User & Service passwords and disable all accounts
□ 20. Domain admin only to server
□ 21. Build new DCs with old names and IPs
□ 22. Move to Production
□ 23. Raise forest functional level
□ 24. Raise domain functional level
□ 25. Get KMS running
□ 26. Bring Exchange Online
□ 27. Delete all accounts in Disabled OU
□ 28. Build new DHCP servers and transfer roles from old DHCP servers
□ 29. Renew Root Certificate Authority
□ 30. Renew Sub Certificate Authority
□ 31. Renew all Servers Certificates
□ 32. Renew all Public Certificates
□ 33. Reset local password on servers
□ 34. Move Exchange to O365
□ 35. Change domain function level to 2016
□ 36. Servers
  □ a. Restore Backup in Triage vlan
  □ b. Install AMP / Sentinel One
  □ c. Update VM Hardware
  □ d. Update VM Tools
  □ e. Install Windows patches

Next steps . . . .Prioritization . . . Servers/PC's



System prioritization workflow v1 – draft

11/10/2020

Hardware Davis/Cornell

Receive System Status

Determine # of Devices

Install Devices

Is Customer Functional?

Complete

Infrastructure Fossen

Password Change with Vendor

Restore/Rebuild System

System has a clean scan and updated MS Patches?

Notify Attestation of Screen Shot of Clean Scan and updated Patches

Notify HW of next System on-line

Systems Completed: 1) Mmodal, 2) Epiphany, 3) Kronos, 4) Sectra, 5) Mosaiq, 6) OBIX, 7) Johnson Control, 8) Corepoint, NetSmart, Metacase, Bbraun, Tguard, HCI Insights, Roche, SpaceLabs, SafeNSound,

On Deck – Epic, Email, Vocera, many many more ☺

Imaging Chancellor

Prepare Image

Deploy Image

Let HW know image deployed

Start next Image

Imaged areas – 1) Radiology, 2) CTC, 3) FBC, 4) Training Rooms – Calypso, Discover, Admiral, Enterprise, 5) CHC, 6) Ivanti Management Console

Attestation Gaede

Prepare Attestation Form

Contact Vendor with Attestation form

Document Attestation complete in Teams

Department

Determine number of Essential Devices

Plan the Device Strategy with HW Team

Systems Completed: 1) Mmodal, 2) Epiphany, 3) Kronos, 4) Sectra, 5) Mosaiq, 6) OBIX, 7) Johnson Control, 8) Corepoint, NetSmart, Metacase, Bbraun, Tguard, HCI Insights, Roche, SpaceLabs, SafeNSound,

On Deck – Epic, Email, Vocera, many many more ☺

Imaged areas – 1) Radiology, 2) CTC, 3) FBC, 4) Training Rooms – Calypso, Discover, Admiral, Enterprise, 5) CHC, 6) Ivanti Management Console

Coordinating the PC availability as Servers come online . . .

Next Steps . . . Process Server side

1) Dirty VLAN to the
2) Staging VLAN to the
3) Clean VLAN

1) Restore clean good known back-up in the clean environment (Staging VLAN)
2) Full installation and system scan with Cisco's AMP and Kivu's SentinelOne (Staging VLAN)
3) Full Microsoft patching (Staging VLAN)
4) Move server to clean VLAN – Production environment (Clean VLAN)
5) System Owner validation
6) Release for Production Use

Next Steps . . . First Milestone – Network

1) Build out Active Directory in the clean VLAN (complete 11/04/2020)
2) Build out new Domain Controllers on the clean VLAN (complete 11/05/2020)

Next Steps . . . First Goal – Device Side

1) Rebuilt or Replaced 2500 PC's

   A. Replace about ~680 Windows 7 PC's or legacy PC's with Windows 10

      I. New Image on new Windows 10 devices

   B. Rebuild by Reimaging all remaining Windows 10 devices (~2000 devices 45 minute – 1.5 hour process)

   C. No exceptions – including offsite PC's

Next Steps . . . First Goal – Device Side

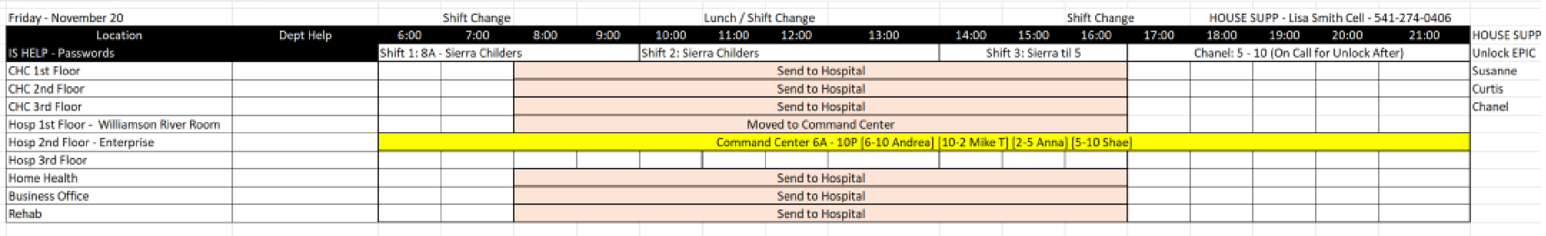
1) Deployed 42 iPads for Haiku and Canto
2) Set up User Access for Haiku/Canto
3) Set up scanners, printers, camera's (Patient Access)
4) Set up remote access to Asante with Cisco DUO (two Factor Authentication) for Epic Back-entry
   A. Billing
   B. HIM, Coding, Medical Records
   C. Patient Access
   D. Lab, Rad, Rx, Cardio

Next Steps . . . 3rd Party

1) Pyxis (disconnect from network and then work with vendor to determine compromise before reconnecting)
2) Diagnostic Imaging – CT, MR, Xray, US, etc. (work with each vendor and assess compromise and reconnection process)
3) Smart Pumps – engage Bioengineering and Vendor to assess compromise

Next Steps . . . First Goal – End User

- 100% strong password change with a minimum of 13 characters
    - Active Directory
    - All Servers/Vendors
    - All VPN’s
    - EMR’s
        - Epic
        - Home Health – NetSmart
        - Elekta Mosaiq
    - All 150 other systems



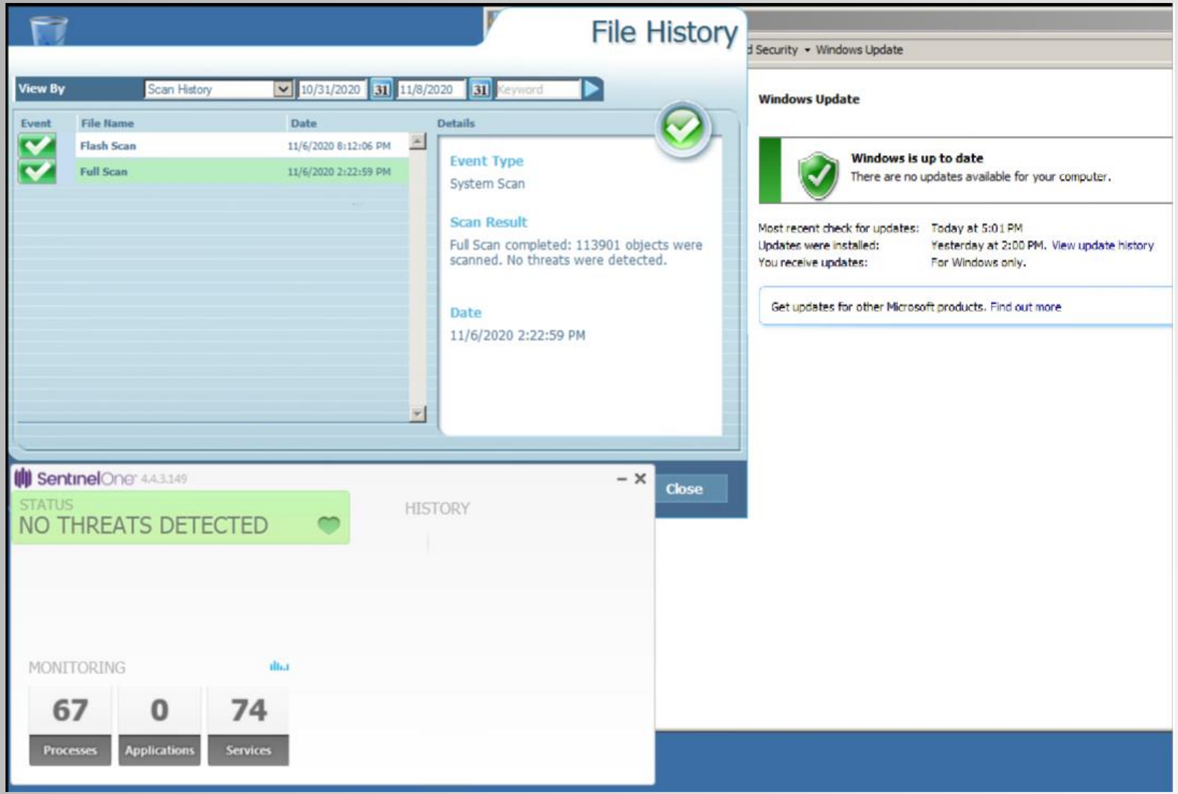
Friday - November 20			Shift Change				Lunch / Shift Change					Shift Change		HOUSE SUPP - Lisa Smith Cell - 541-274-0406				
Location	Dept Help	6:00	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	HOUSE SUPP
IS HELP - Passwords		Shift 1: 8A - Sierra Childers				Shift 2: Sierra Childers				Shift 3: Sierra til 5			Chanel: 5 - 10 (On Call for Unlock After)					Unlock EPIC
CHC 1st Floor				Send to Hospital														Susanne
CHC 2nd Floor				Send to Hospital														Curtis
CHC 3rd Floor				Send to Hospital														Chanel
Hosp 1st Floor - Williamson River Room				Moved to Command Center														
Hosp 2nd Floor - Enterprise		Command Center 6A - 10P [6-10 Andrea] [10-2 Mike T] [2-5 Anna] [5-10 Shae]																
Hosp 3rd Floor																		
Home Health				Send to Hospital														
Business Office				Send to Hospital														
Rehab				Send to Hospital														

Next Steps . . . First Clinical System – Cancer Treatment Center

1) Restore Elekta – MOSAIQ – Radiation Oncology
2) Restore Elekta – MOSAIQ – Medical Oncology
3) Ray Station

- Systems recovered in clean vlan on the evening of 11/07/2020 and in Production environment 11/09/2020

Next Steps . . . Clinical System – Communication with Vendors



View By: Scan History | 10/31/2020 | 11/8/2020 | Keyword

Event	File Name	Date
✓	Flash Scan	11/6/2020 8:12:06 PM
✓	Full Scan	11/6/2020 2:22:59 PM

Details

Event Type
System Scan

Scan Result
Full Scan completed: 113901 objects were scanned. No threats were detected.

Date
11/6/2020 2:22:59 PM

Windows Update

Windows is up to date
There are no updates available for your computer.

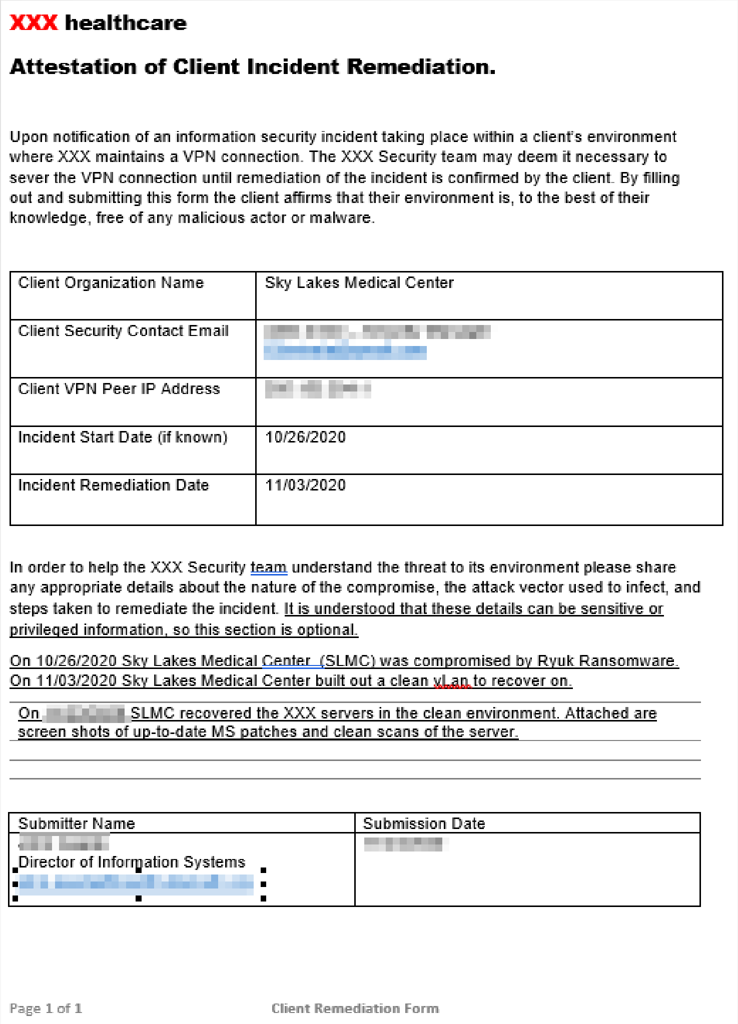
Most recent check for updates: Today at 5:01 PM
Updates were installed: Yesterday at 2:00 PM. View update history
You receive updates: For Windows only.

Get updates for other Microsoft products. Find out more

STATUS
NO THREATS DETECTED

MONITORING

67	0	74
Processes	Applications	Services



XXX healthcare

Attestation of Client Incident Remediation.

Upon notification of an information security incident taking place within a client's environment where XXX maintains a VPN connection. The XXX Security team may deem it necessary to sever the VPN connection until remediation of the incident is confirmed by the client. By filling out and submitting this form the client affirms that their environment is, to the best of their knowledge, free of any malicious actor or malware.

Client Organization Name	Sky Lakes Medical Center
Client Security Contact Email	[redacted]
Client VPN Peer IP Address	[redacted]
Incident Start Date (if known)	10/26/2020
Incident Remediation Date	11/03/2020

In order to help the XXX Security team understand the threat to its environment please share any appropriate details about the nature of the compromise, the attack vector used to infect, and steps taken to remediate the incident. It is understood that these details can be sensitive or privileged information, so this section is optional.

On 10/26/2020 Sky Lakes Medical Center (SLMC) was compromised by Ryuk Ransomware. On 11/03/2020 Sky Lakes Medical Center built out a clean vLan to recover on.

On [redacted] SLMC recovered the XXX servers in the clean environment. Attached are screen shots of up-to-date MS patches and clean scans of the server.

Submitter Name	Submission Date
[redacted] Director of Information Systems [redacted]	[redacted]

Page 1 of 1 Client Remediation Form

Next Steps . . . First Clinical System – Epic Connection with Asante - MOU

1) Asante Health System to build out reconnection steps and criteria for SLMC and AHS
2) Build documentation
3) Agree on the Memorandum of Understanding (MOU)
   A. 3rd Party Clean Bill of Health
   B. Annual Risk Assessments with PEN Testing
   C. Incident Notification – Timely
   D. NIST v2 Framework – Security Posture/Culture

Next Steps . . . First Enterprise Clinical System - Epic

2) Restore 3rd Party Systems to support Epic
   G. BCA – Business Continuity Access
   H. EPS – Epic Print Servers
   I. Go Anywhere – Secure File Transfer
   J. Right Fax – Faxing
   K. Citrix – Asante and SLMC

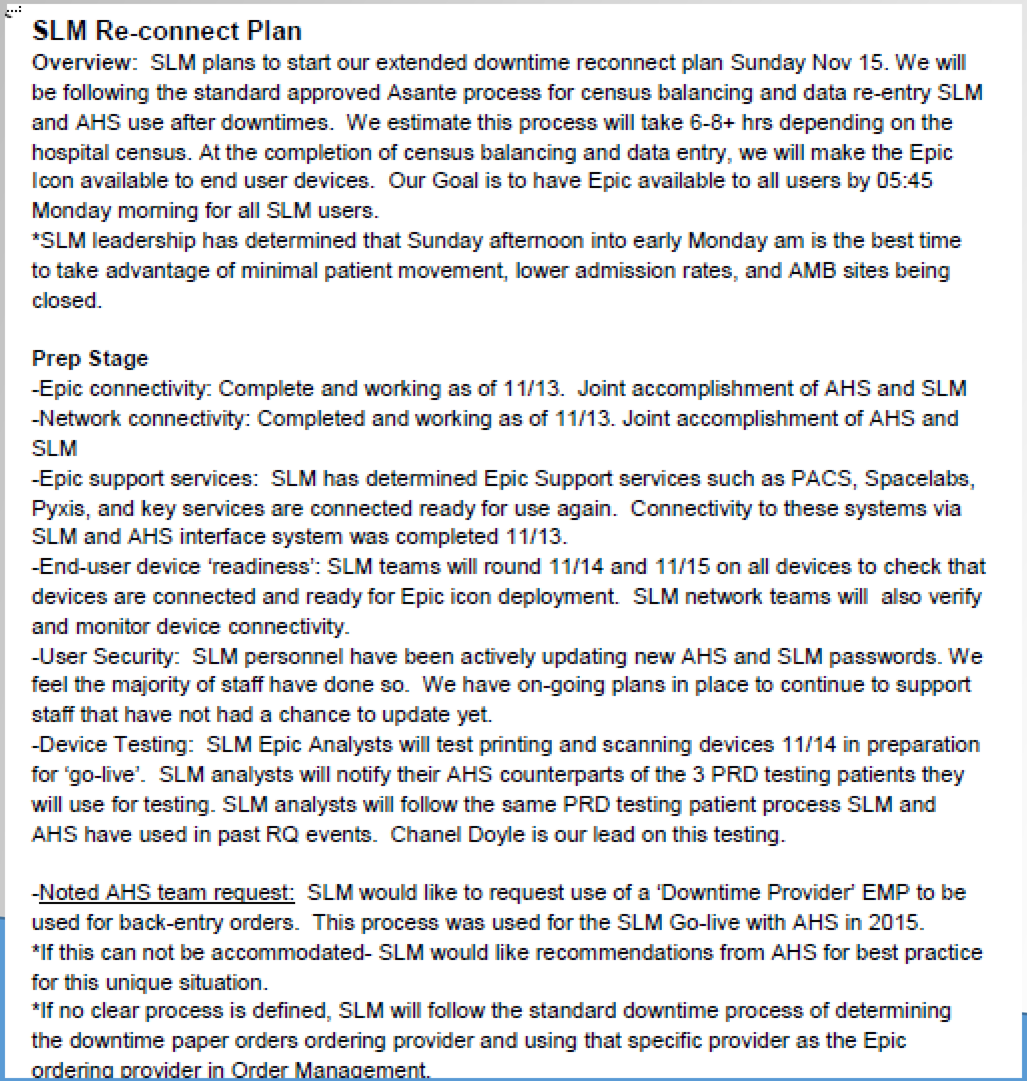
Epic GO LIVE 11/18/2020 @2230

Next Steps . . . First Enterprise Clinical System - Epic

1) Restore Epic to full clinical use enterprise wide
2) Restore 3rd Party Systems to support Epic
   A. Interface Engine – Corepoint (Lyniate)
   B. Pyxis – Pharmacy
   C. Sectra PACS – Diagnostic Imaging
   D. Data Innovations (DI), Remisol, RALS (POC), HCLL, LabCorp, Mayo, Reliance – Laboratory
   E. Cardiac Monitoring Equipment – SpaceLabs
   F. EKG's - Epiphany

Epic GO LIVE 11/18/2020 @2230

Next Steps . . . Documented GO LIVE plan to Asante



SLM Re-connect Plan

Overview: SLM plans to start our extended downtime reconnect plan Sunday Nov 15. We will be following the standard approved Asante process for census balancing and data re-entry SLM and AHS use after downtimes. We estimate this process will take 6-8+ hrs depending on the hospital census. At the completion of census balancing and data entry, we will make the Epic Icon available to end user devices. Our Goal is to have Epic available to all users by 05:45 Monday morning for all SLM users.

*SLM leadership has determined that Sunday afternoon into early Monday am is the best time to take advantage of minimal patient movement, lower admission rates, and AMB sites being closed.

Prep Stage

-Epic connectivity: Complete and working as of 11/13. Joint accomplishment of AHS and SLM

-Network connectivity: Completed and working as of 11/13. Joint accomplishment of AHS and SLM

-Epic support services: SLM has determined Epic Support services such as PACS, Spacelabs, Pyxis, and key services are connected ready for use again. Connectivity to these systems via SLM and AHS interface system was completed 11/13.

-End-user device 'readiness': SLM teams will round 11/14 and 11/15 on all devices to check that devices are connected and ready for Epic icon deployment. SLM network teams will also verify and monitor device connectivity.

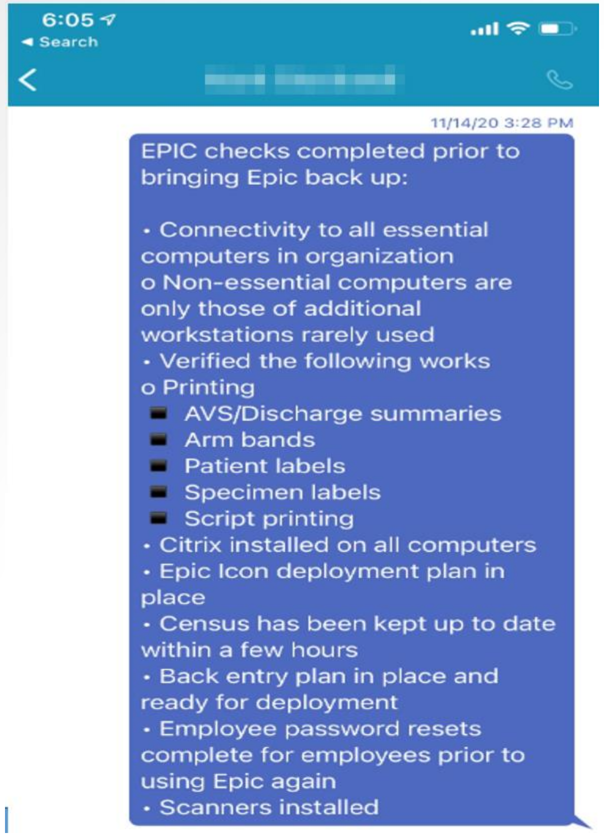
-User Security: SLM personnel have been actively updating new AHS and SLM passwords. We feel the majority of staff have done so. We have on-going plans in place to continue to support staff that have not had a chance to update yet.

-Device Testing: SLM Epic Analysts will test printing and scanning devices 11/14 in preparation for 'go-live'. SLM analysts will notify their AHS counterparts of the 3 PRD testing patients they will use for testing. SLM analysts will follow the same PRD testing patient process SLM and AHS have used in past RQ events. Chanel Doyle is our lead on this testing.

-Noted AHS team request: SLM would like to request use of a 'Downtime Provider' EMP to be used for back-entry orders. This process was used for the SLM Go-live with AHS in 2015.

*If this can not be accommodated- SLM would like recommendations from AHS for best practice for this unique situation.

*If no clear process is defined, SLM will follow the standard downtime process of determining the downtime paper orders ordering provider and using that specific provider as the Epic ordering provider in Order Management.



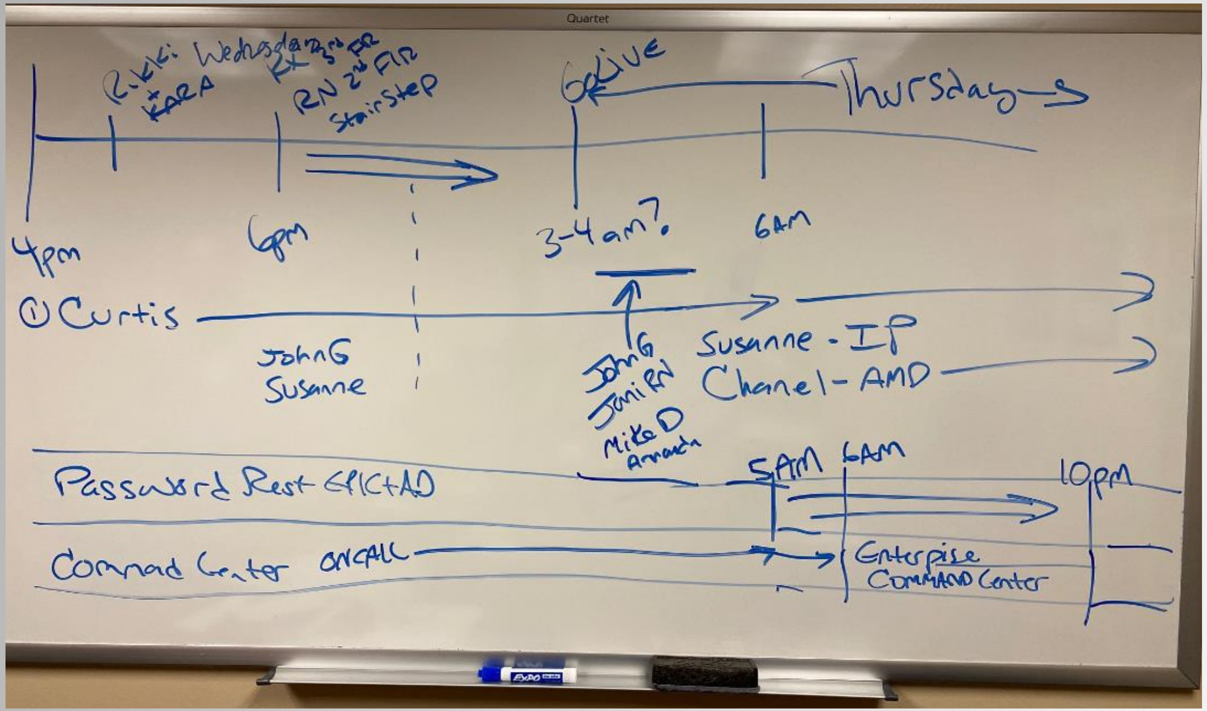
[redacted]

11/14/20 3:28 PM

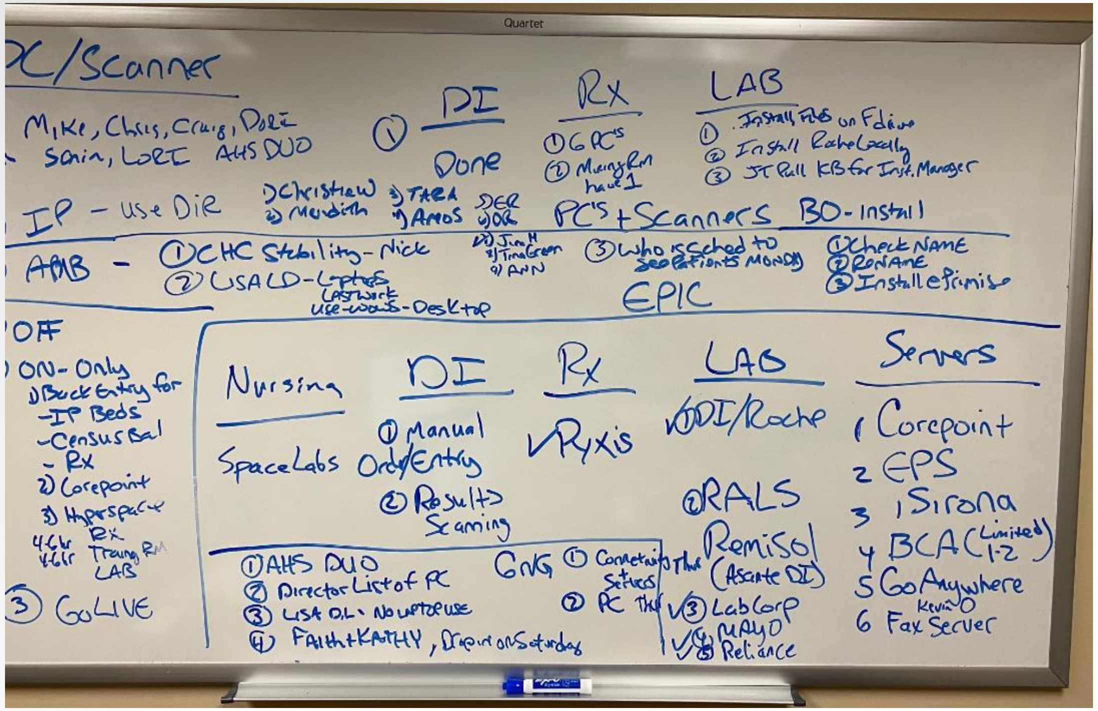
EPIC checks completed prior to bringing Epic back up:

• Connectivity to all essential computers in organization
o Non-essential computers are only those of additional workstations rarely used
• Verified the following works
o Printing
▪ AVS/Discharge summaries
▪ Arm bands
▪ Patient labels
▪ Specimen labels
▪ Script printing
• Citrix installed on all computers
• Epic Icon deployment plan in place
• Census has been kept up to date within a few hours
• Back entry plan in place and ready for deployment
• Employee password resets complete for employees prior to using Epic again
• Scanners installed

Next Steps . . . GO LIVE- Epic
Coverage and Planning - Whiteboarding



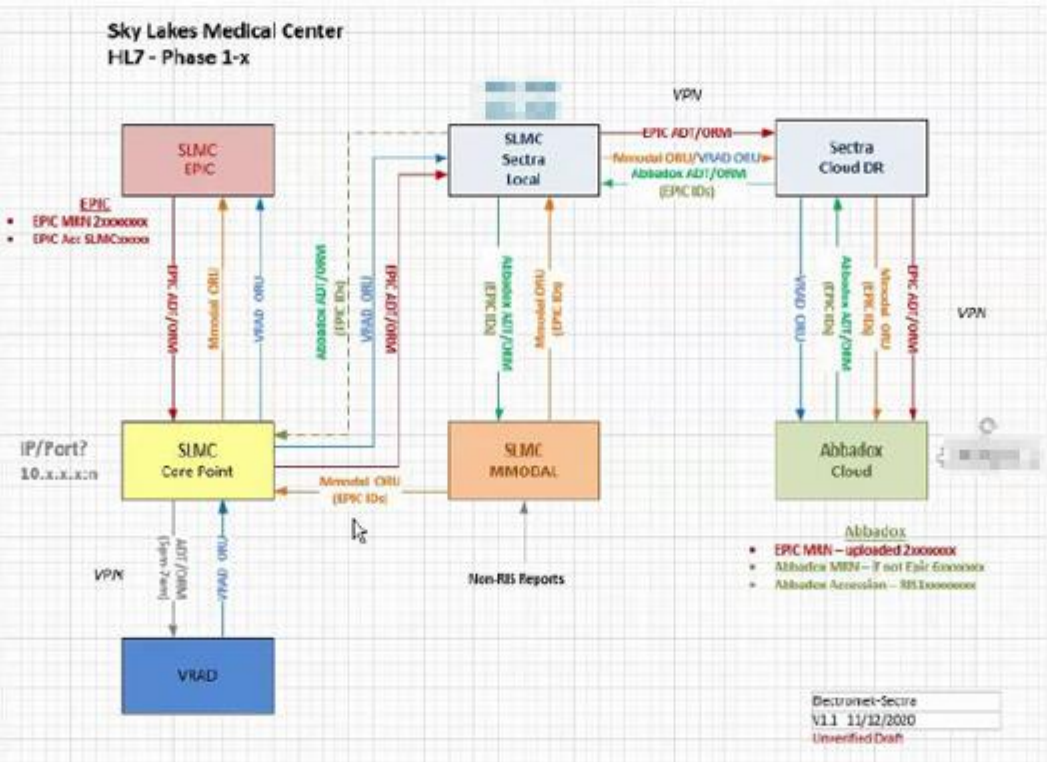
Epic – Support – Team coverage – Command Center . . .

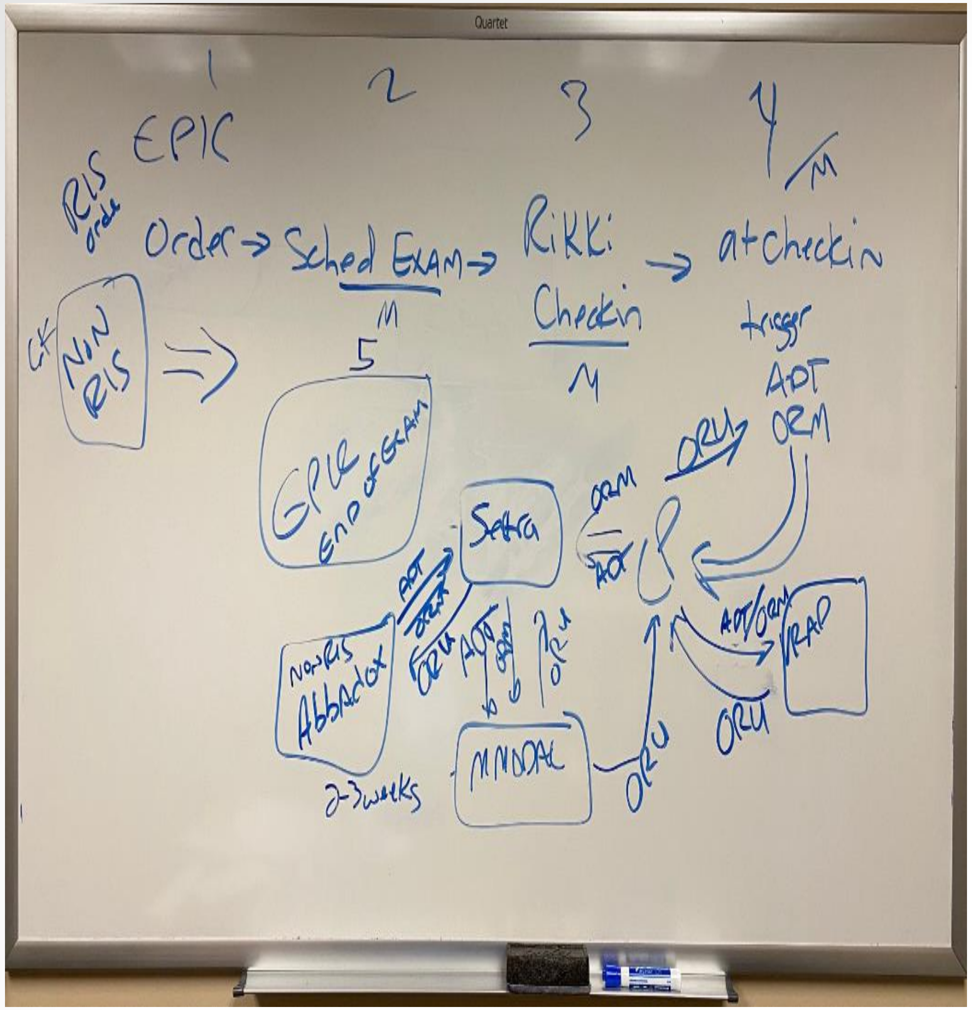


Epic systems planning . . .

People, processes and technology . . .

Next Steps . . . GO LIVE- Sectra PACS - Whiteboarding





Build out an integrated PACS solution to work with Epic . . .

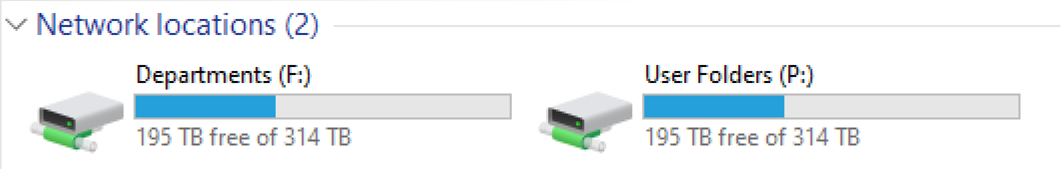
Next Steps . . . GO LIVE- Epic Back-Entry of Data

1) Back-Entry for GO-LIVE – Registration, Nursing, Pharmacy
   B. All patients in a bed had to have the paper record keyed into Epic – Lab, Rad, Cardio, Dietary
   C. All orders entered and up to date

Clinical Back-Entry Team – MD's, RN's etc.

100% downtime – full paper

- Epic offline 23 days – Go LIVE Wednesday November 18th @ 2230
- Email restored about day 30 to a pilot group
- P drive/ F drive

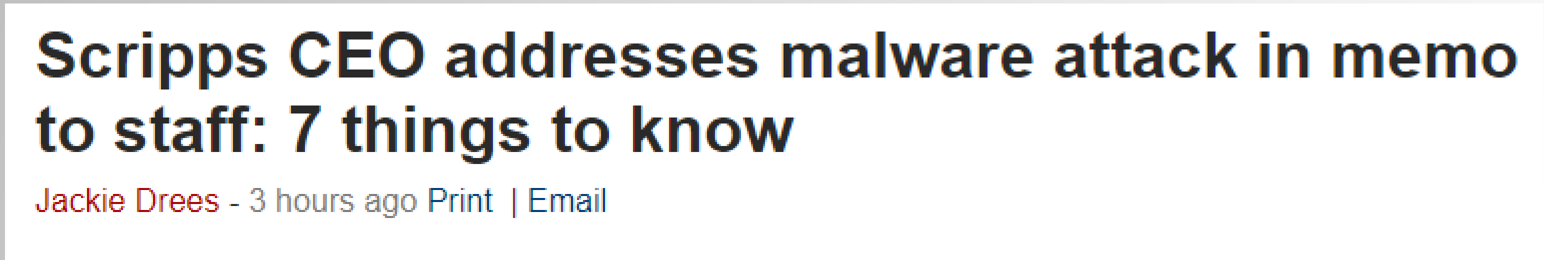


Network locations (2)

Departments (F:)
195 TB free of 314 TB

User Folders (P:)
195 TB free of 314 TB

Scripps hit May 01 . . . Now day 20. . .



Scripps CEO addresses malware attack in memo to staff: 7 things to know

Jackie Drees - 3 hours ago Print | Email

2. . . . Mr. Van Gorder thanked employees for their continued support: "I've been asked how much more you can all take on top of what you have already done over the past 15 months and more," he wrote. "My answer is Scripps will always do what is necessary to care for our patients first so that means we will do whatever it takes to do so – and you are. **Using our manual systems for a couple of hours is one thing – it's another altogether to do it for days** – but you are."

https://www.beckershospitalreview.com/cybersecurity/scripps-ceo-addresses-malware-attack-in-memo-to-staff-7-things-to-know.html?origin=CEOE&utm_source=CEOE&utm_medium=email&utm_content=newsletter&oly_enc_id=6455D6976723I0A accessed 05122021.

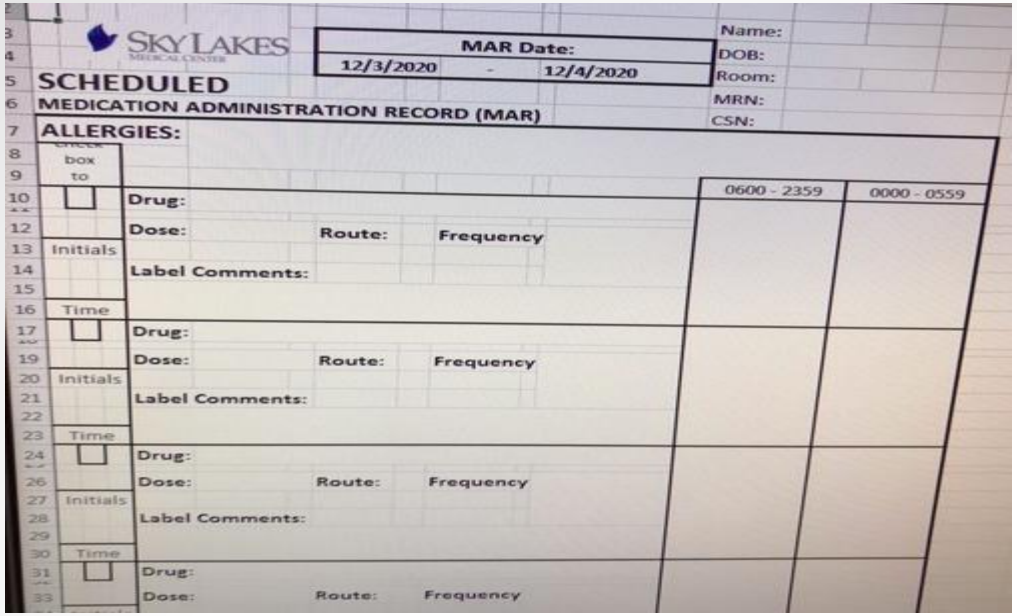
100% downtime – full paper

Problem : Managing 'Medication Administration Records' without the EMR.

Challenge was that during our downtime, we had to create and manage a paper written Medication Administration Record (MAR).

The paper process was very labor intensive to manage and edit multiple medications per patient. This MAR only covered a 24hr time span, so it had to be transcribed and verified to a new record each day. Without additional staff (unit secretaries), this task had to be added to the RN role. The transcription and verification was taking 30-45minutes per patient.

Solution- Nursing Educator and Clindoc Analyst Brad N developed an Excel Spreadsheet to manage the MAR. Medications were recorded and verified once a shift on this tool. This allowed us to do edits instead of complete re-writes of the paper, allowed for standardization (look, feel, structure, etc); reduced hand-written errors; provided printed text instead of hand-writing; and allowed for clean record keeping. Nursing still printed the MAR to document on and work from but keeping the medication orders current on the Spreadsheet made the task much more manageable and safer. Ultimately, this allowed us to regain some functions that the EMR normally provides.



SKY LAKES MEDICAL CENTER

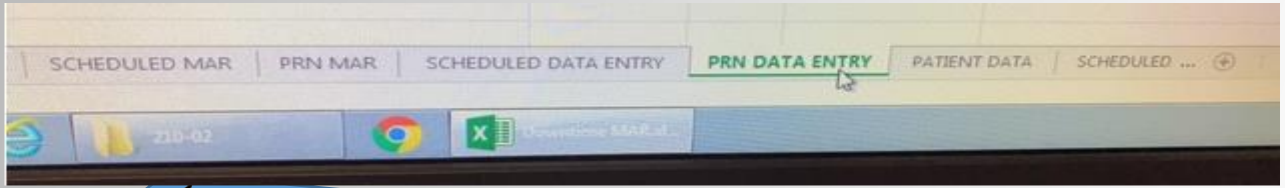
MAR Date: 12/3/2020 - 12/4/2020

Name:
DOB:
Room:
MRN:
CSN:

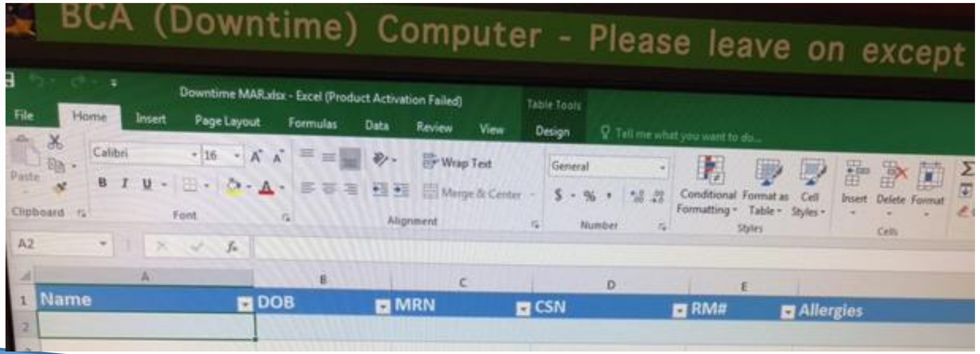
SCHEDULED
MEDICATION ADMINISTRATION RECORD (MAR)

ALLERGIES:

Check box to		0600 - 2359	0000 - 0559
□	Drug:		
Initials	Dose: Route: Frequency		
	Label Comments:		
Time			
□	Drug:		
Initials	Dose: Route: Frequency		
	Label Comments:		
Time			
□	Drug:		
Initials	Dose: Route: Frequency		
	Label Comments:		
Time			
□	Drug:		
	Dose: Route: Frequency		



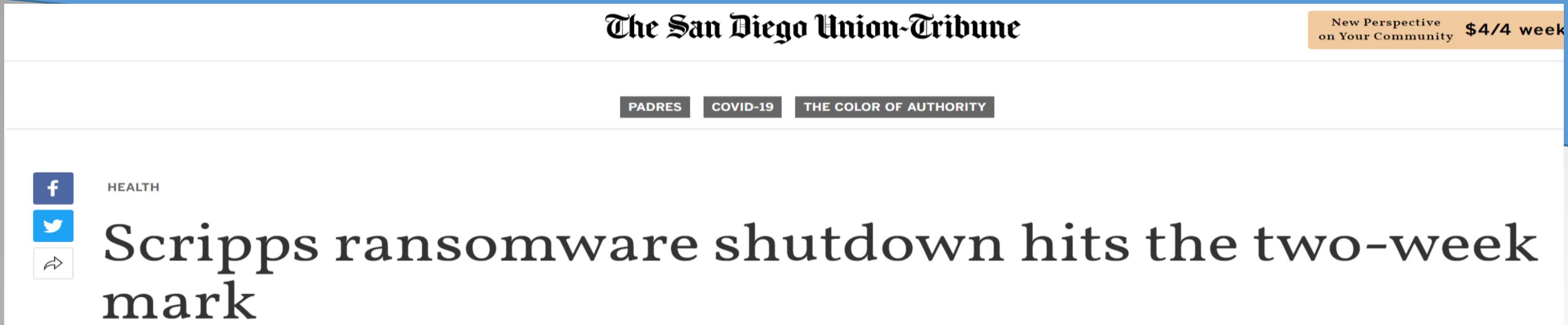
SCHEDULED MAR | PRN MAR | SCHEDULED DATA ENTRY | PRN DATA ENTRY | PATIENT DATA | SCHEDULED ...



BCA (Downtime) Computer - Please leave on except

Downtime MAR.xlsx - Excel (Product Activation Failed)

Name	DOB	MRN	CSN	RM#	Allergies



The San Diego Union-Tribune

HEALTH

Scripps ransomware shutdown hits the two-week mark

“I cannot stress this enough, every minute we are there we feel like we are playing with our license,” one nurse said, adding that many have been advising their own family members to stay away. “We are all buying malpractice insurance at this time.”

While it was clear that many were out of practice using more manual methods, the 60-year-old said that, in her experience, there was plenty of safety-related redundancy. “Everything was double- and triple-checked,” she said.

Scripps ransomware shutdown hits the two-week mark - The San Diego Union-Tribune (sandiegouniontribune.com)accessed 05/15/2021

Clinical Impacts . . .

1) The Medical Record–
   A. Patient History (find phone numbers and call family)
   B. How to correctly place an order (EMR has all the steps)
   C. Bins to transport tubes in the ED

2) Communication-
   A. Between Shifts – relied on ‘white boards’
   B. Between departments – Lab, Rx, Imaging, Nursing
   C. Staffing – relied on texting and cell phones

Operations Impacts . . .

- Paper
  - Prescription pads – availability and enough
  - Toner for all the copying
  - Correct documentation – Signatures, Diagnosis, Dates, Orders
  - Enterprise wide impact – Billing, Invoices for Non-Patient AR etc,

- Providers who have only had training on EMR's, now paper

- Massive backlog of paper
  - To be scanned (HIM)
  - Coding/Billing delays – looking for paper
  - Clinics – MD signatures

Clinical Impacts . . .

“We have worked downtime out of our processes” Ron Woita, acting CNO, Sky Lakes Medical Center (03/08/2021)

Back-Entry of Data Importance …

1) Post live back entry: Affects all operations –
   A. Billing
   B. HIM – Medical Record
   C. Clinical data continuity
      I. Discrete data
      II. Scanned records
   D. Reporting
      A. Gap in Data
      B. Regulatory reporting

Potential Data Loss . . .

- Diagnostic Imaging Images
- 40 TB over more than a decade
- 1.5 million studies
  - Potentially unrecoverable images

- Data not stored on the P and F drives

Financial Impacts . . .

Experience is the hardest kind of teacher.
It gives you the test first and the lesson afterward.

- Oscar Wilde

PFS Operations: Pre Ryuk

Sunday, October 25, 2020

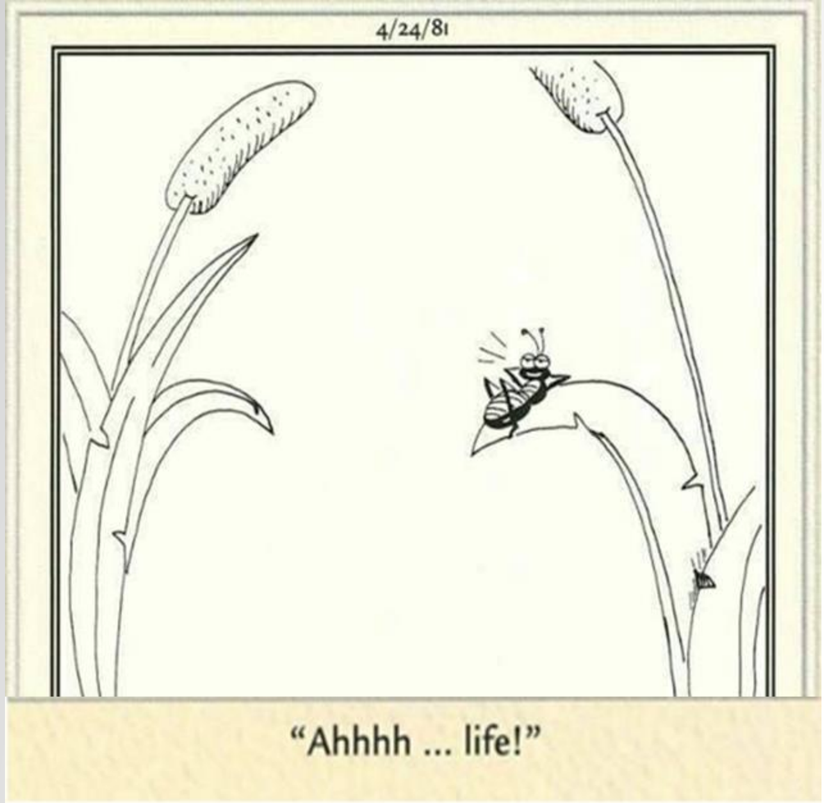
	Total AR Days	Total AR Dollars (M)	Candidate for Billing Days Claims Pending Days	Candidate for Billing Dollars (M) Claims Pending Dollars (K)
HB	56.2	$92.7	14.5	$23.9
PB	36.8	$4.5	0.7	$86.0

	Outstanding Claims Days	Outstanding Claims Dollars (M)
HB	26.5	$43.7
PB	20.7	$2.5

	% AR <60 Days	Clean Claim Rate
HB	79.7%	87.5%
PB	71.0%	88.9%

October 25, 2020

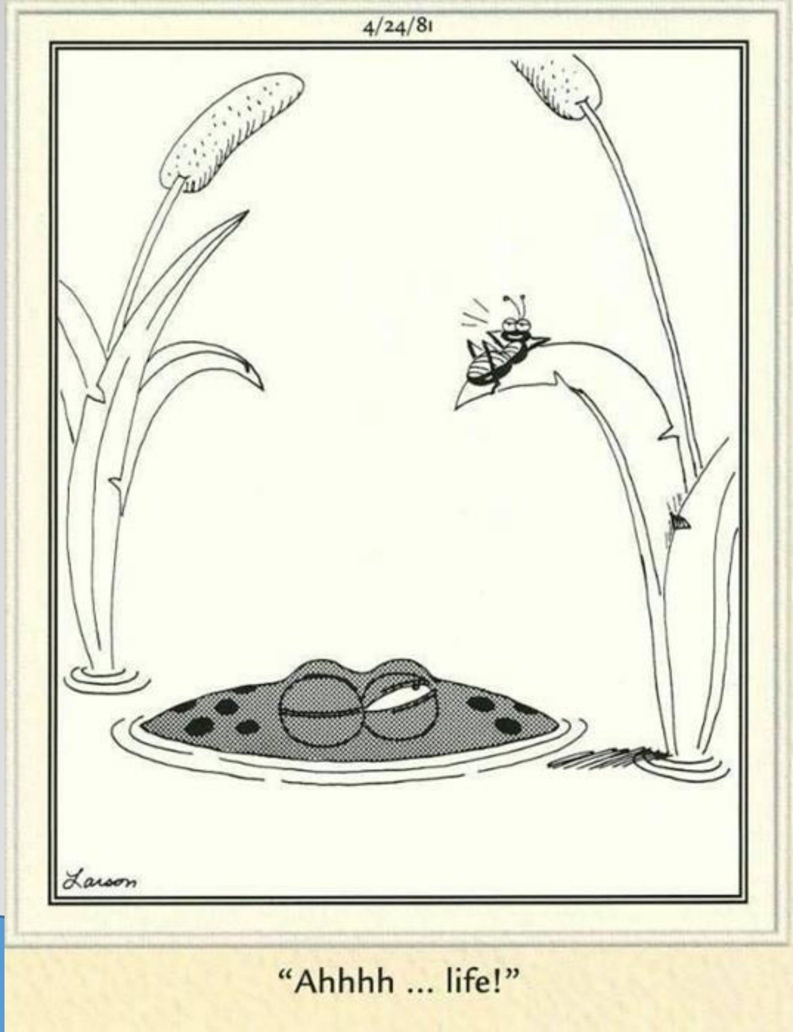
Our view of the world…



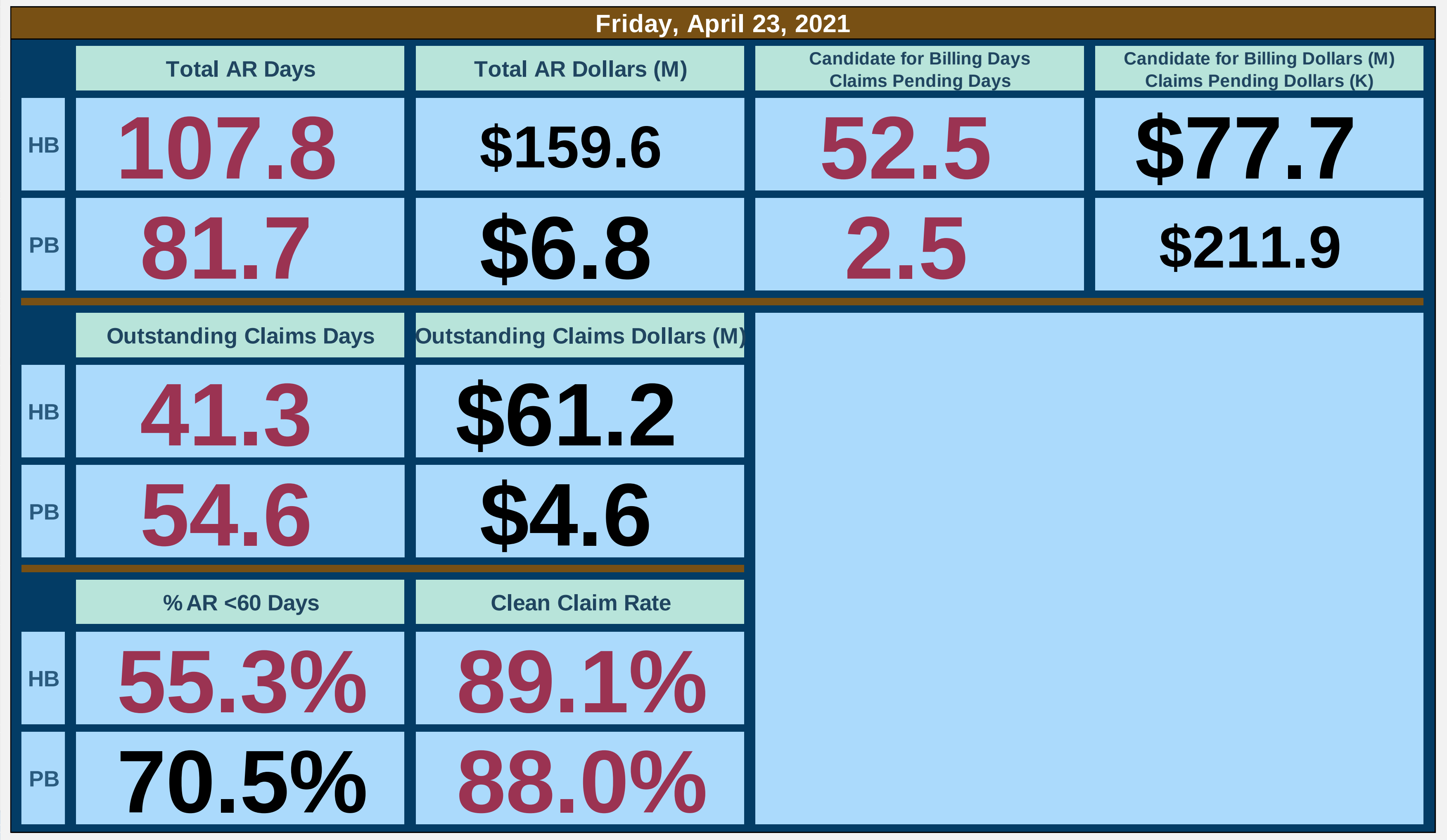
"Ahhhh ... life!"

October 26, 2020

The world's view of us…



PFS Operations: Post Ryuk



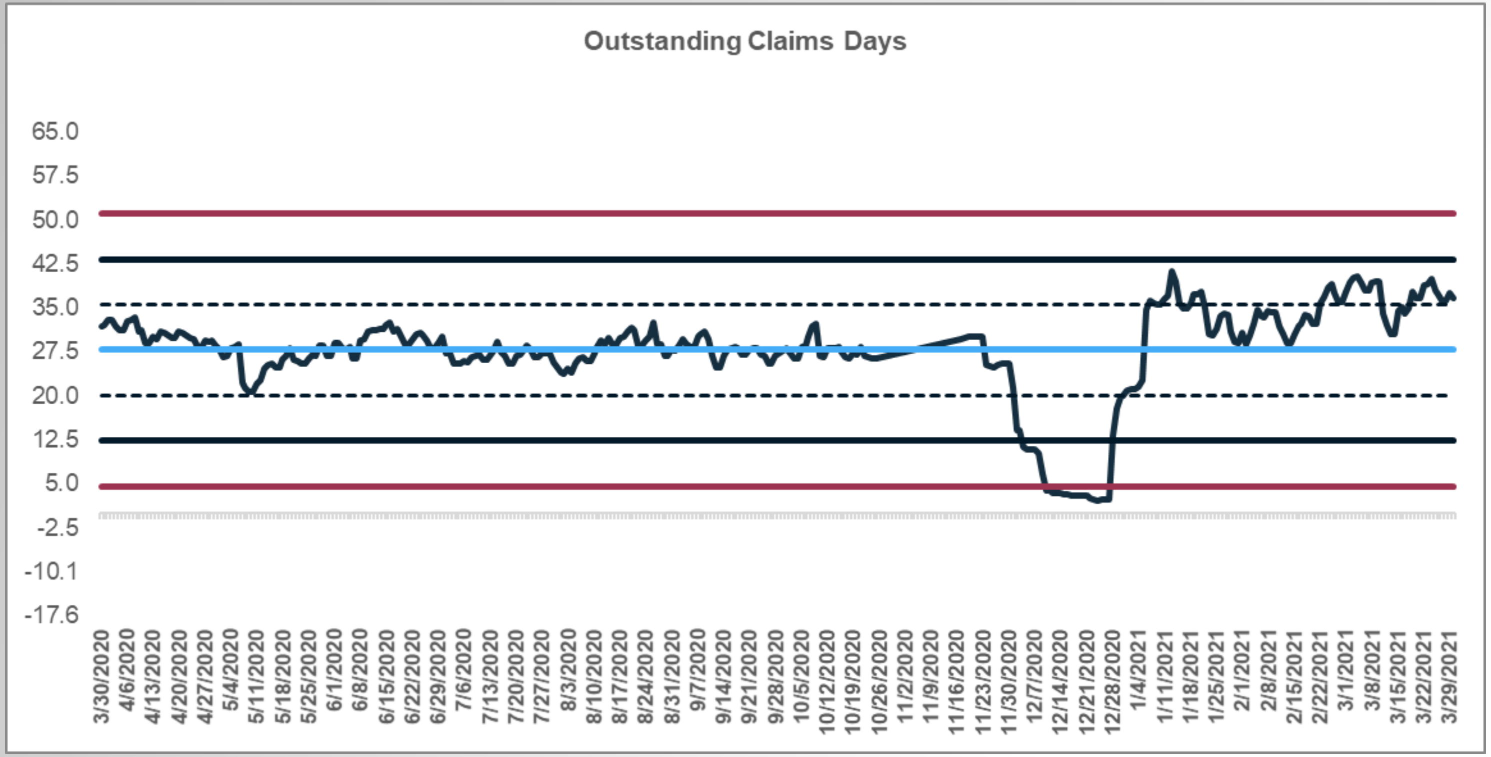
Friday, April 23, 2021

	Total AR Days	Total AR Dollars (M)	Candidate for Billing Days Claims Pending Days	Candidate for Billing Dollars (M) Claims Pending Dollars (K)
HB	107.8	$159.6	52.5	$77.7
PB	81.7	$6.8	2.5	$211.9

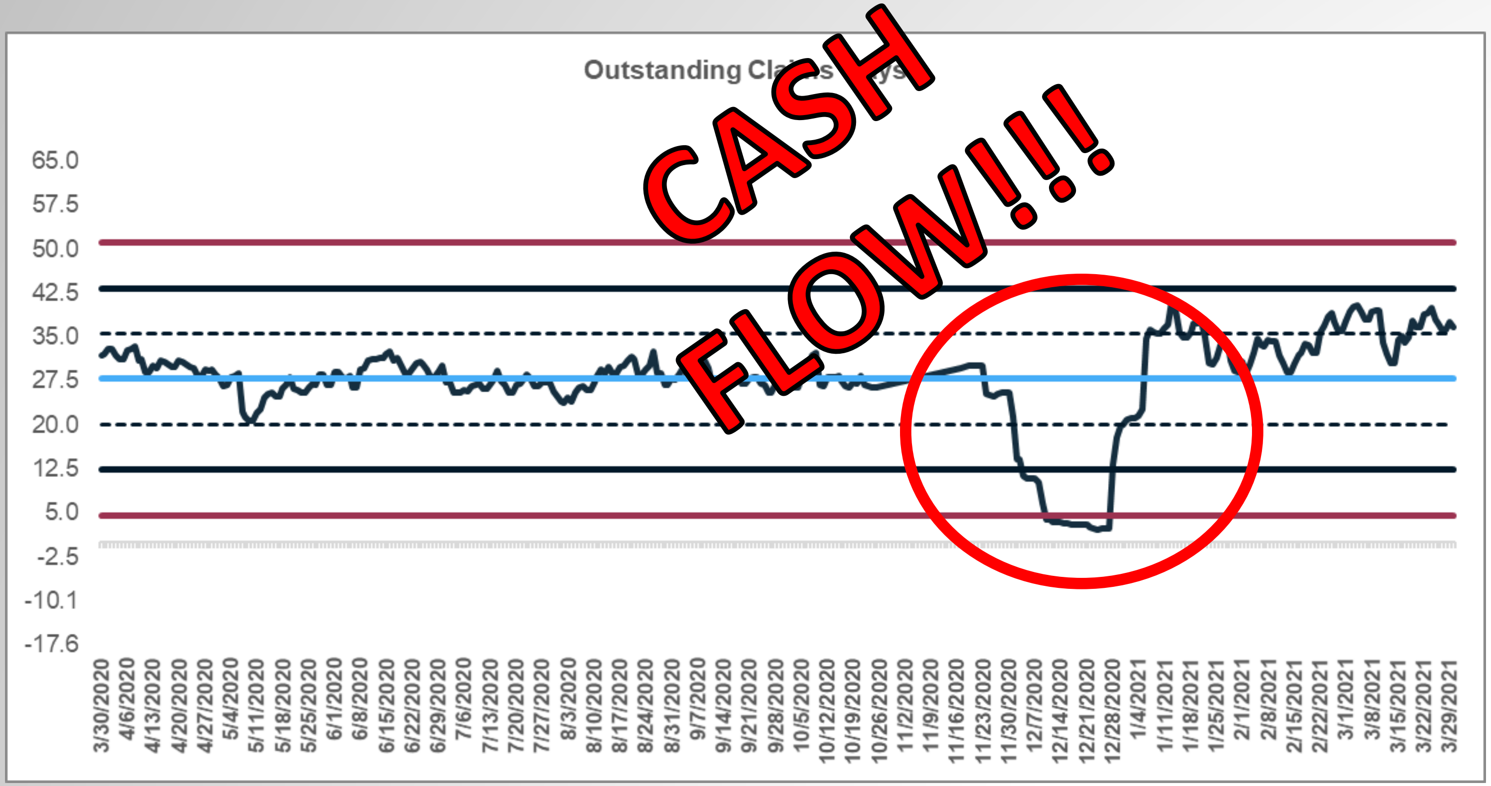
	Outstanding Claims Days	Outstanding Claims Dollars (M)
HB	41.3	$61.2
PB	54.6	$4.6

	% AR <60 Days	Clean Claim Rate
HB	55.3%	89.1%
PB	70.5%	88.0%

Critical Metric: Post Ryuk



Be Prepared



- Outstanding Claims drop from 30.2 days to 4.6 days – ONE MONTH!

PFS Ryuk Time-Line

- **Timeline**
  - 10/25/20 Operations normal
  - 10/26/20 – 11/17/20 No Activity
    - No billing
    - No follow-up
    - No posting
    - No customer statements
  - 11/18/20 Epic up
  - 11/23/20 Posting resumes
  - 12/28/20 1st post disaster claim run
  - 1/4/20 1st statement run
  - 1/6/21 Autopayment issue
  - 1/7/21 Autopayment issue resolved
  - 3/19/21 Remaining disaster claims released

Recovery

First Action To Take…

- Get on the phone and contact major payors

First Oops…

- No access to contacts stored in Outlook

Recovery

Tip

Make sure you have all contacts saved on another device or (dare I say it) written in a Rolodex

Recovery

Question

If Epic was restored on 11/17/20, why didn’t billing resume until 12/28/20?

Answer

There were no claims ready to be billed.

- Billing System
  - Interfaces needed to be re-established
- Charge Capture
  - There was about one month of back-logged charges to be entered into Epic
- Coding
  - Coding continued to be out of commission until encoder was restored

And…

Recovery (continued)

We didn’t know what would happen when we turned everything back on.

- No other Epic facility had done a total shut down
- Epic was not sure what would happen

Recovery (continued)

When we flipped the switch, everything worked!

Recovery (continued)

Once we were up and running:

- Clinical Departments
  - Were able to begin charging current services
- Coding was able to begin coding current claims

The challenge was the back-logged charges

- Paper records needed to be entered into Epic
  - Limited staff available
  - Questionable documentation
    - **Critical Finding: Many of our clinical staff had never documented on paper!**

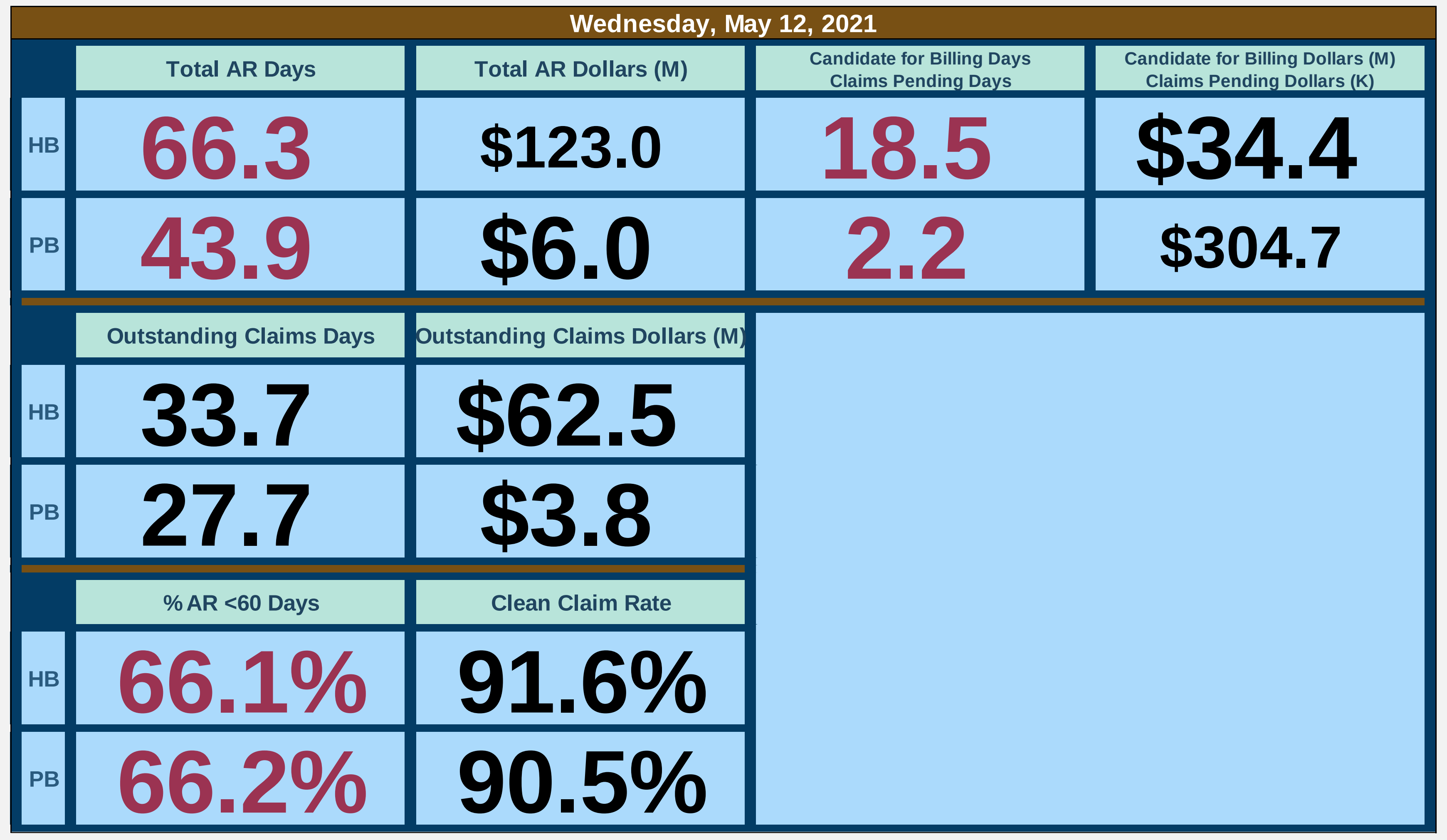
Recovery (continued)

The Unintended Opportunity

From January to the end of March we had two groups of claims to work

- New claims (starting in January)
- Aged claims
  - We used this time to aggressively work AR >90 Days
    This enabled us to concentrate on the Down-Time claims when they were released

PFS Operations: Recovery



Wednesday, May 12, 2021

	Total AR Days	Total AR Dollars (M)	Candidate for Billing Days Claims Pending Days	Candidate for Billing Dollars (M) Claims Pending Dollars (K)
HB	66.3	$123.0	18.5	$34.4
PB	43.9	$6.0	2.2	$304.7

	Outstanding Claims Days	Outstanding Claims Dollars (M)
HB	33.7	$62.5
PB	27.7	$3.8

	% AR <60 Days	Clean Claim Rate
HB	66.1%	91.6%
PB	66.2%	90.5%

Summary . . .

Recovery . . . All other systems

1) Restore from good known backups (Cohesity) – all other systems
2) For SLMC that is about 650 servers and 150 applications
3) Complete recovery of systems in March 2021 (Oct 26, 2020 – March 2021)

Complete Recovery – May 2021

- 6 months for full recovery
  - All billing sent
  - All systems online
  - All Medical Records complete

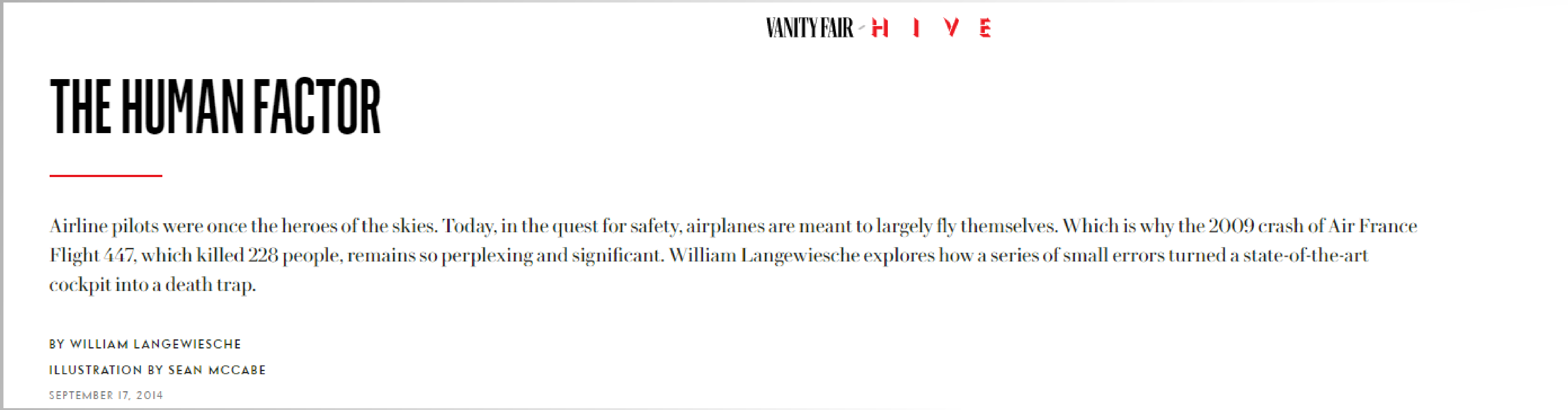
How do we prevent this?

- Good Backups
- SOC – 24/7/365 Security Operations Center
- Education – 1st Line of defense

- Playbook
- Paper
- Learned something about rapid deployment of systems

The resiliency of good, hard working people and partnership companies . . .

Technology to solve the problem?



VANITY FAIR HIVE

THE HUMAN FACTOR

Airline pilots were once the heroes of the skies. Today, in the quest for safety, airplanes are meant to largely fly themselves. Which is why the 2009 crash of Air France Flight 447, which killed 228 people, remains so perplexing and significant. William Langewiesche explores how a series of small errors turned a state-of-the-art cockpit into a death trap.

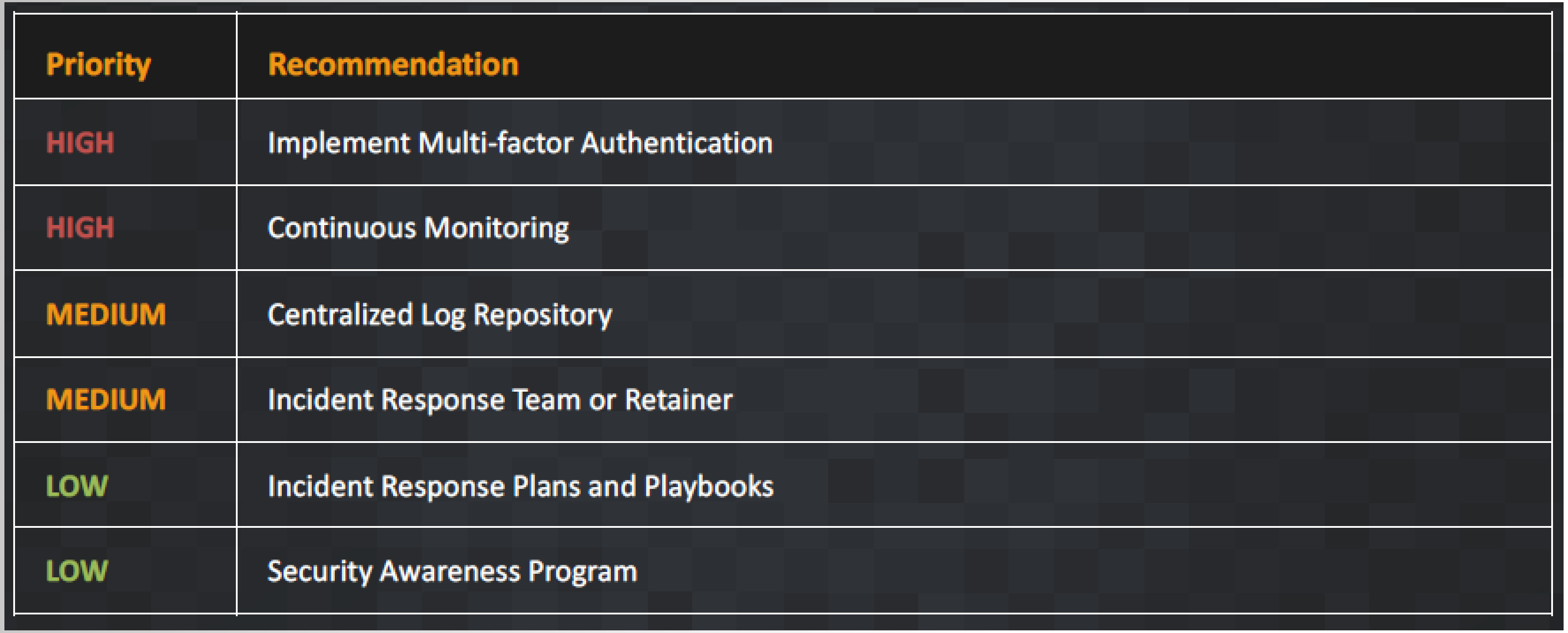
BY WILLIAM LANGEWIESCHE

ILLUSTRATION BY SEAN MCCABE

SEPTEMBER 17, 2014

Should Airplanes Be Flying Themselves? | Vanity Fair accessed 05032021 written by William Langewiesche, illustration by Sean Mccabe Sept 17,2014

Summary of Strategic Recommendations



Priority	Recommendation
HIGH	Implement Multi-factor Authentication
HIGH	Continuous Monitoring
MEDIUM	Centralized Log Repository
MEDIUM	Incident Response Team or Retainer
LOW	Incident Response Plans and Playbooks
LOW	Security Awareness Program

Q & A