Business Continuity in an All Varian Environment

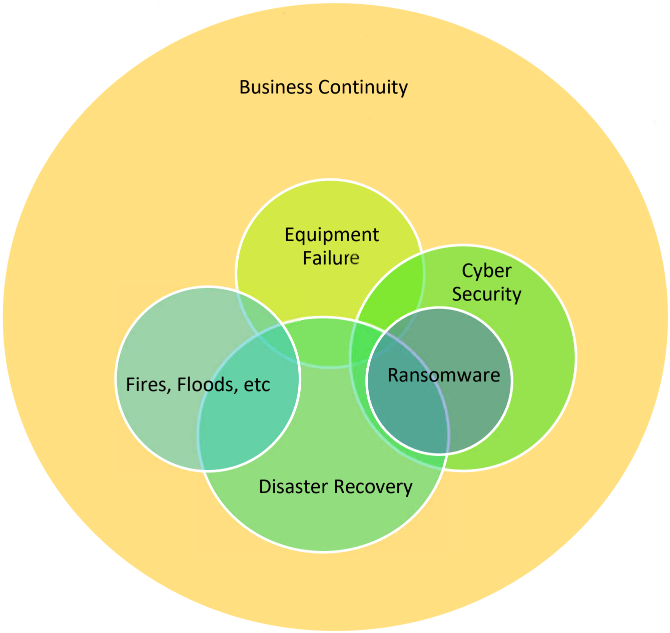
R. Alfredo C. Siochi, PhD, DABR
Department of Radiation Oncology
West Virginia University

WVU Medicine
Radiation Oncology

Conflicts of Interest

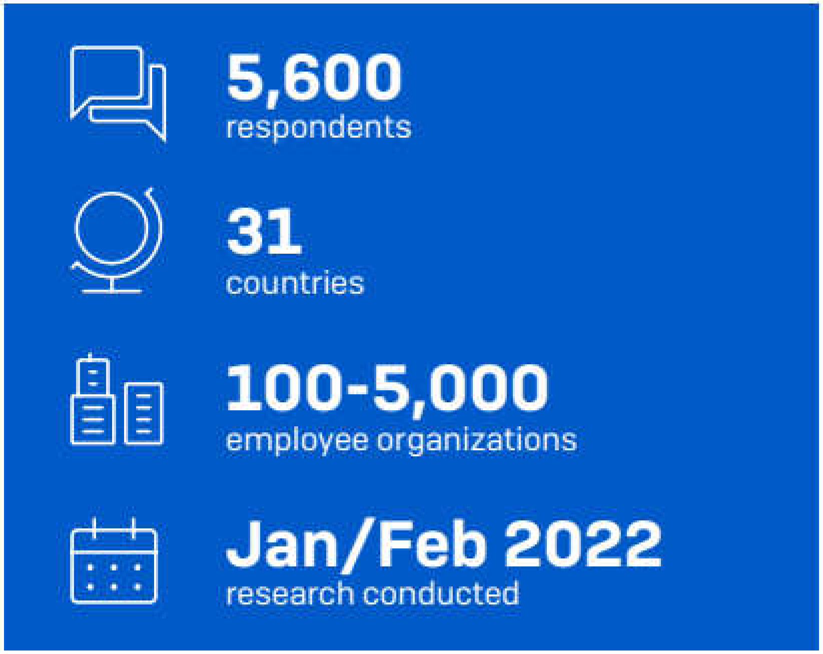
- Not related to this topic
  - Co-founder of Infondrian, LLC
    - Gap fund and Iowa based Grant to Infondrian
    - NIH phase I and phase II STTR grants
  - Various TG, committees, leadership positions in AAPM, ASTRO
- Related to topic
  - We use Varian equipment at our clinic

Focus on Ransomware



Ransomware

Sophos Survey – Ransomware 2022



5,600
respondents

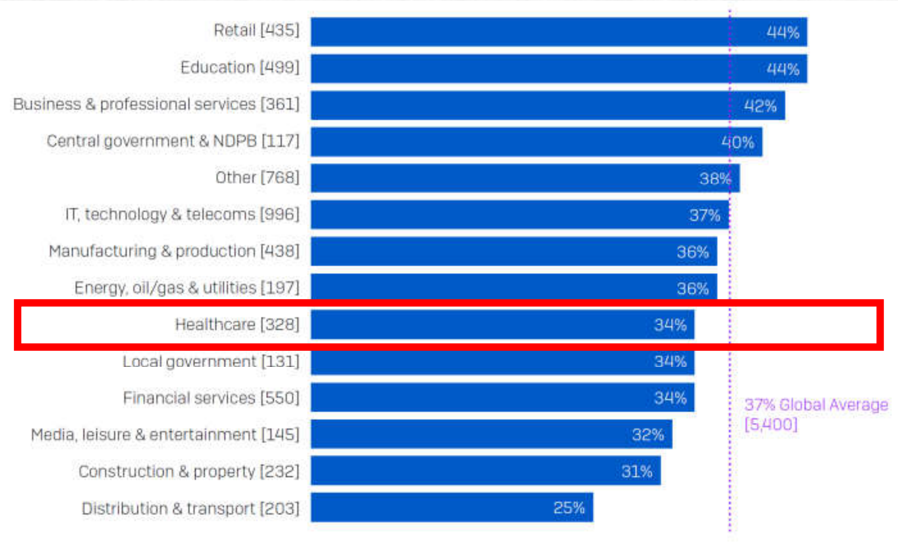
31
countries

100-5,000
employee organizations

Jan/Feb 2022
research conducted

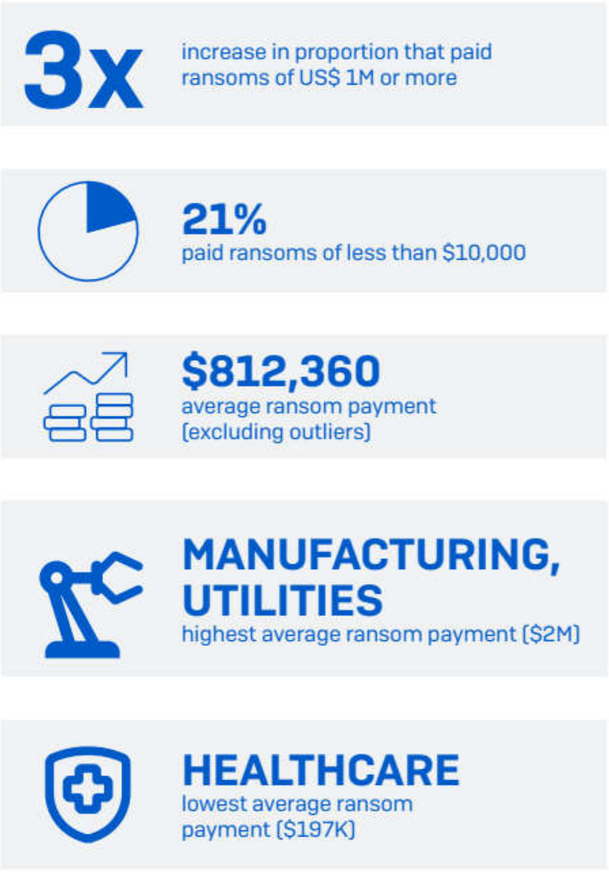
From Reference # 1

Looking at the rate of attacks by sector, we see considerable variation in the rate of attacks using ransomware across different industries with Healthcare falling in around 34% which is just below the global average rate of 37%.



The State of Ransomware – Sophos Cybersecurity Annual Report 2021 **Slide courtesy of Mike Tallhamer**

Ransom payments have increased from 2020 to 2021



3x increase in proportion that paid ransoms of US$ 1M or more

21% paid ransoms of less than $10,000

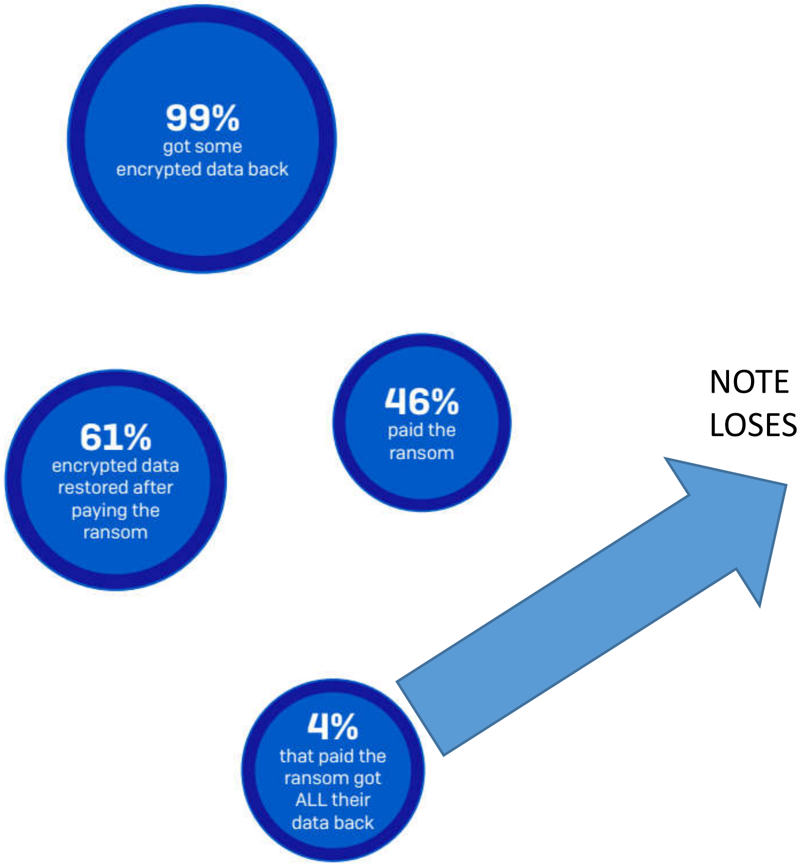
$812,360 average ransom payment (excluding outliers)

MANUFACTURING, UTILITIES highest average ransom payment ($2M)

HEALTHCARE lowest average ransom payment ($197K)

From Reference # 1

Restoring Data after an attack



99% got some encrypted data back

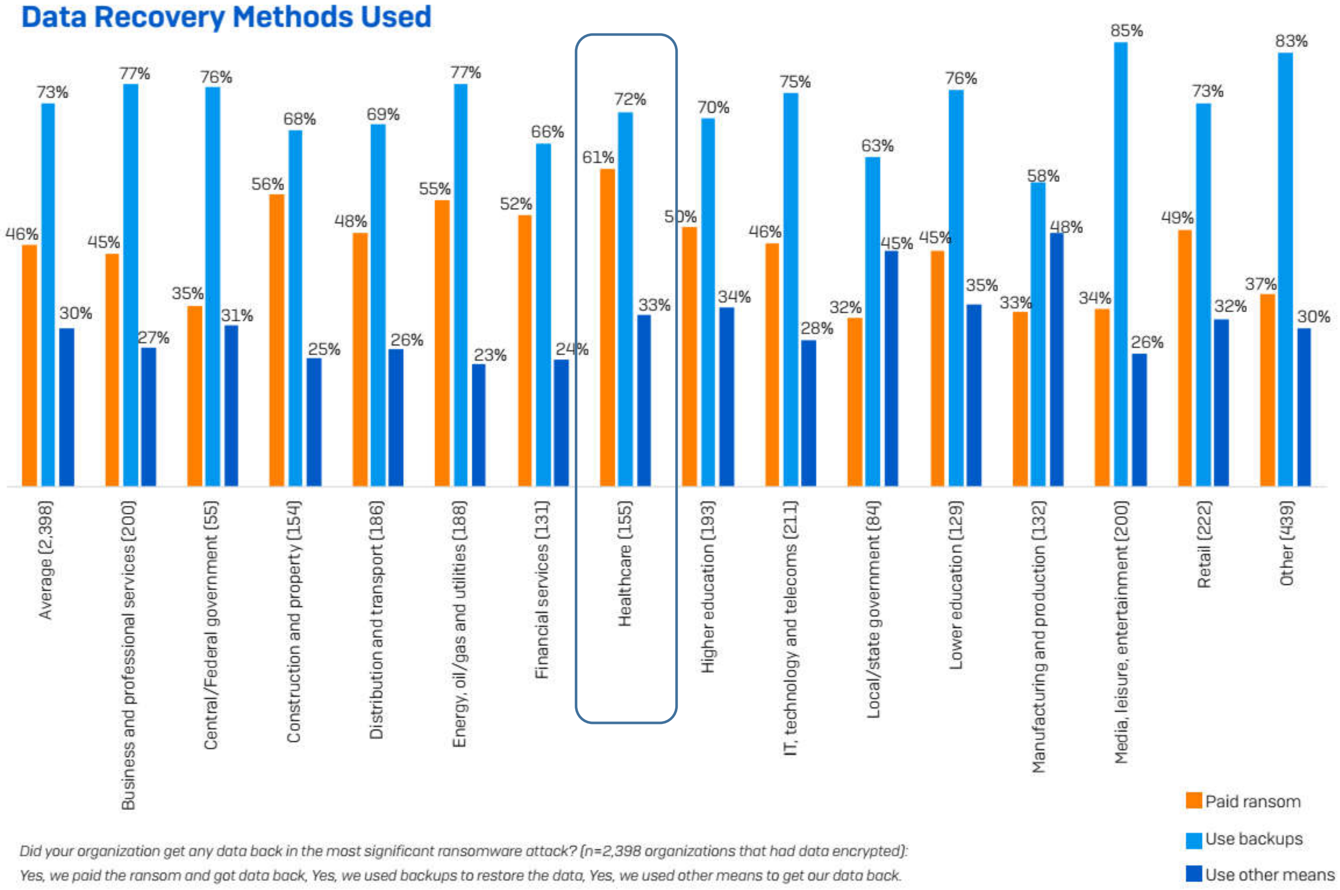
61% encrypted data restored after paying the ransom

46% paid the ransom

4% that paid the ransom got ALL their data back

NOTE – ALMOST EVERYONE LOSES SOME DATA

From Reference # 1



Did your organization get any data back in the most significant ransomware attack? (n=2,398 organizations that had data encrypted): Yes, we paid the ransom and got data back, Yes, we used backups to restore the data, Yes, we used other means to get our data back.

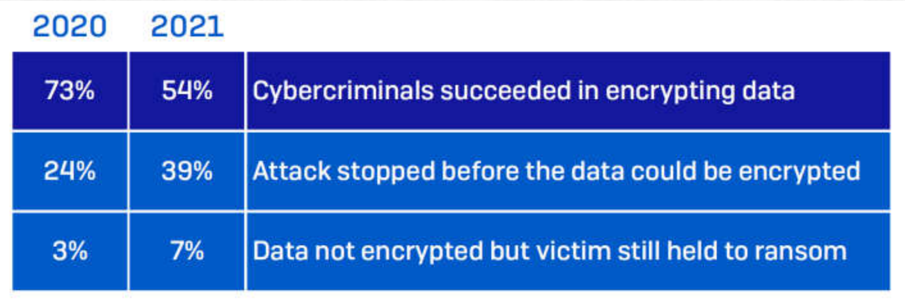
More Backups = less ransom!

From Reference # 1

Ransomware attack success is not simply measured by rate but by other factors

Success rates are up while attack rates are down

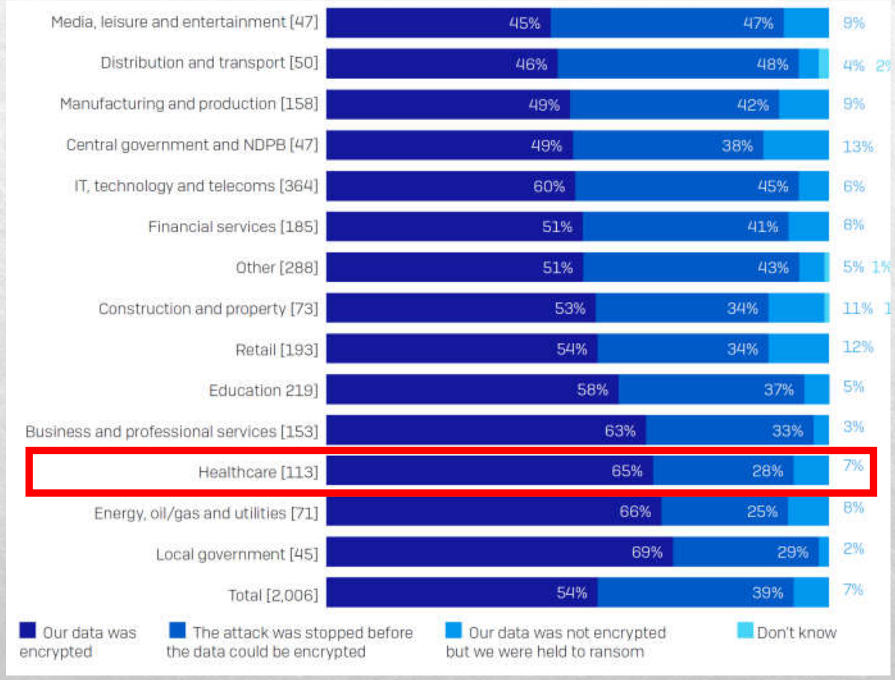
- Encryption events are down
- Extortion rates are up



2020	2021	
73%	54%	Cybercriminals succeeded in encrypting data
24%	39%	Attack stopped before the data could be encrypted
3%	7%	Data not encrypted but victim still held to ransom

The State of Ransomware – Sophos Cybersecurity Annual Report 2021 **Slide courtesy of Mike Tallhamer**

Healthcare experiences a below-average number of attacks. However, attackers succeed in encrypting files in almost two-thirds (65%) of incidents, which is considerably above average.

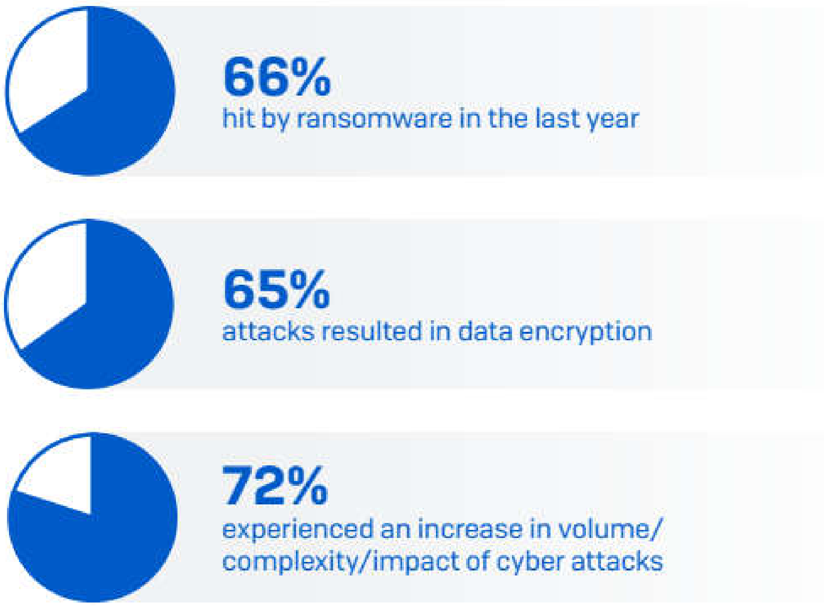


The State of Ransomware – Sophos Cybersecurity Annual Report 2021 **Slide courtesy of Mike Tallhamer**

Attacks are getting worse

Events in 2021

54% in 2020



66%
hit by ransomware in the last year

65%
attacks resulted in data encryption

72%
experienced an increase in volume/complexity/impact of cyber attacks

From Reference # 1

Steps to increase Ransomware Resilience

01

Dispersion

Dispersing your backups across different data stores and media reduces the chance that your backups will be impacted during a ransomware attack

02

Immutable

Keep at least 1 copy of your data on immutable storage media or offline (not always viewed favorably) so that it is unreachable to potential attackers

03

Frequency

Continuously backup your data. The frequency of the data backup will help ensure favorable Recovery Point Objectives (RPO) can be met in the clinic.

04

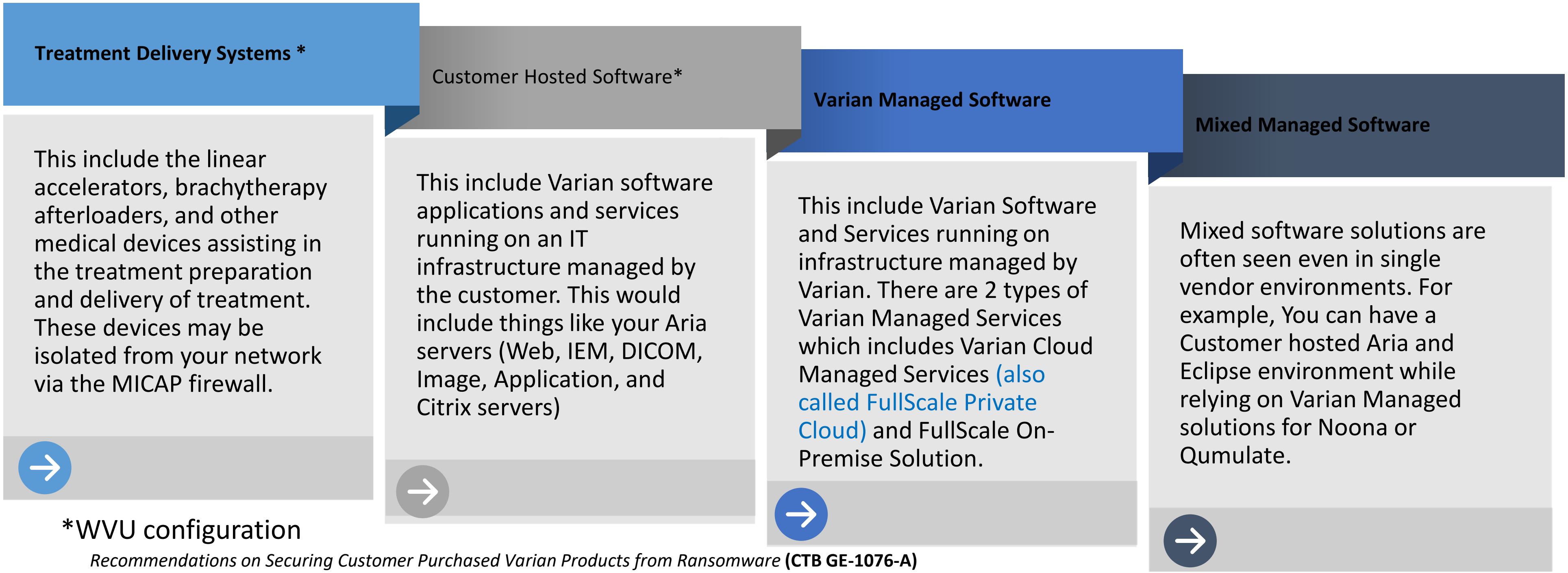
Develop & Test

Develop a disaster recovery (DR) plan and test the recovery workflow at least annually to ensure media storage availability is adequate for clinical operations to continue.

NISTIR 8374 - Ransomware Risk Management: A Cybersecurity Framework Profile, National Institute of Standards and Technology James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

NIST Guide for Conducting Risk Assessments https://www.nist.gov/publications/guide-conducting-risk-assessments **Slide courtesy of Mike Tallhamer**

Ransomware Resilience Means Understanding your Vendor Environment Topology



Treatment Delivery Systems *

This include the linear accelerators, brachytherapy afterloaders, and other medical devices assisting in the treatment preparation and delivery of treatment. These devices may be isolated from your network via the MICAP firewall.

Customer Hosted Software*

This include Varian software applications and services running on an IT infrastructure managed by the customer. This would include things like your Aria servers (Web, IEM, DICOM, Image, Application, and Citrix servers)

Varian Managed Software

This include Varian Software and Services running on infrastructure managed by Varian. There are 2 types of Varian Managed Services which includes Varian Cloud Managed Services (also called FullScale Private Cloud) and FullScale On-Premise Solution.

Mixed Managed Software

Mixed software solutions are often seen even in single vendor environments. For example, You can have a Customer hosted Aria and Eclipse environment while relying on Varian Managed solutions for Noona or Qumulate.

*WVU configuration

Recommendations on Securing Customer Purchased Varian Products from Ransomware **(CTB GE-1076-A)**

Slide courtesy of Mike Tallhamer

Preparing for a ransomware attack

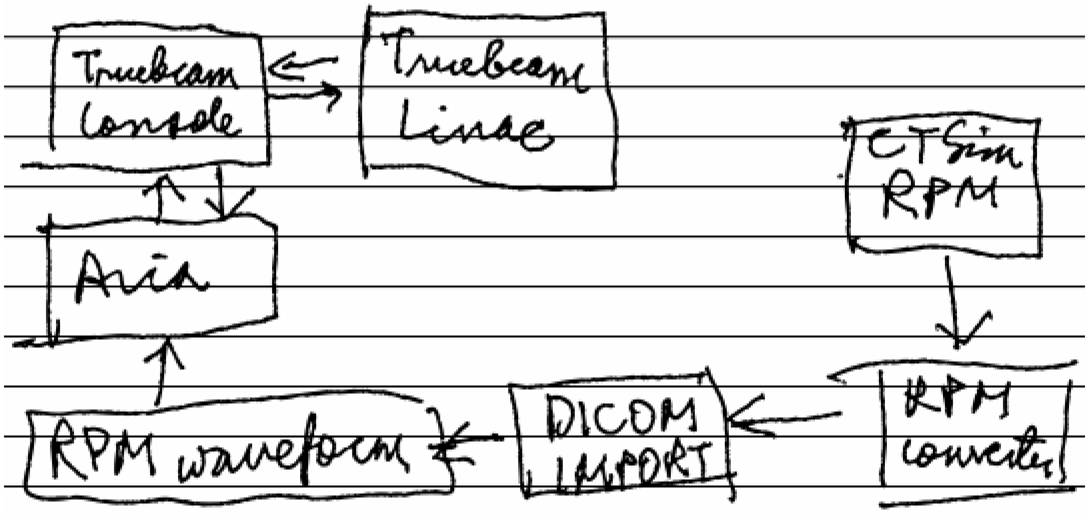
- Identify and protect critical data, systems and devices
- Detect ransomware events as early as possible
  - Preferably before ransomware is deployed
- Response and Recovery Processes in place.

From Reference # 2a

IDENTIFY

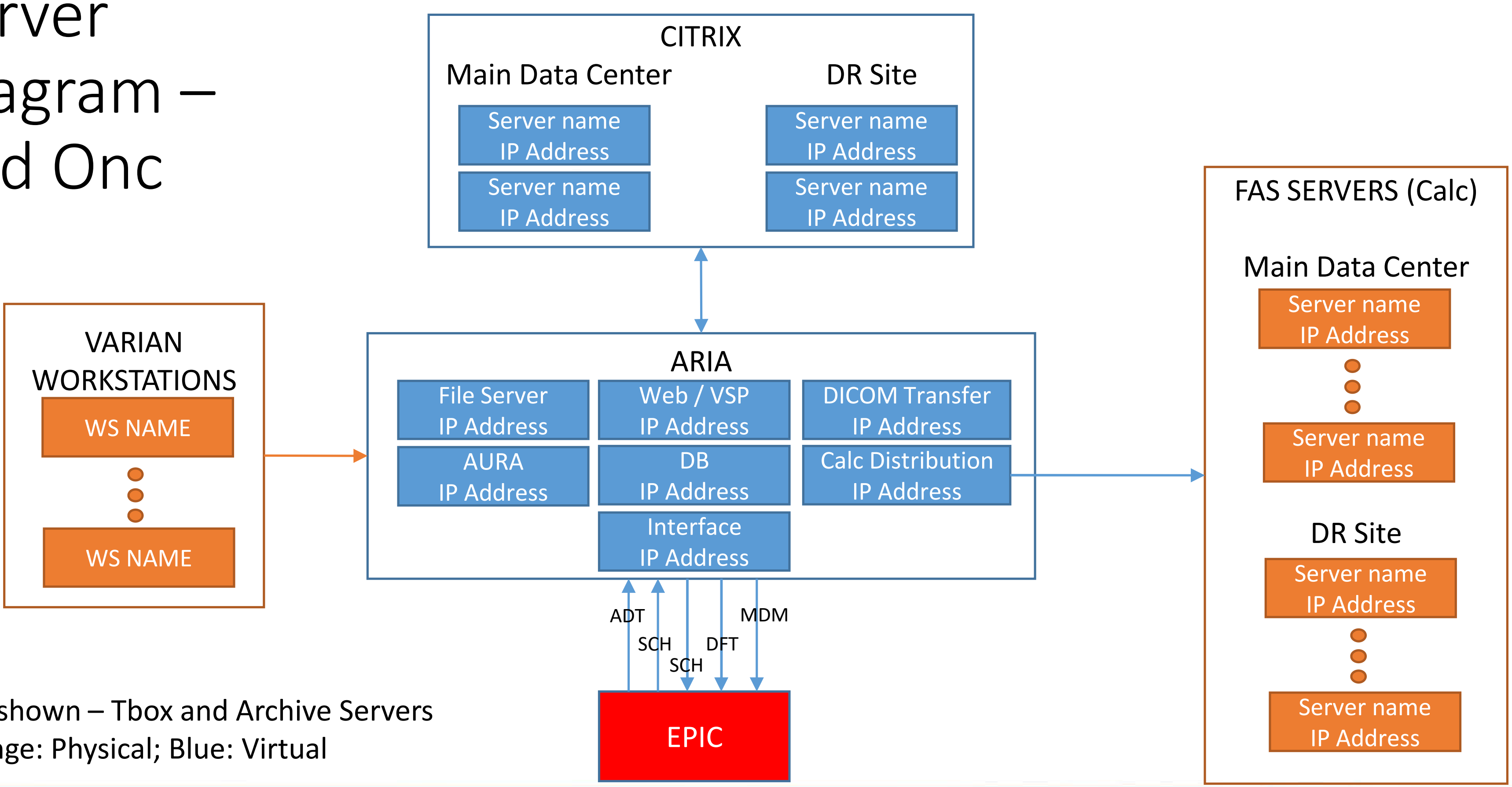
- Inventory of
  - devices and systems
  - Software platforms / applications
- Mapping of
  - Data flows
  - Organizational communication
- Catalog of
  - External information systems

INVENTORY: Do a quick sketch of the devices and the data flows.



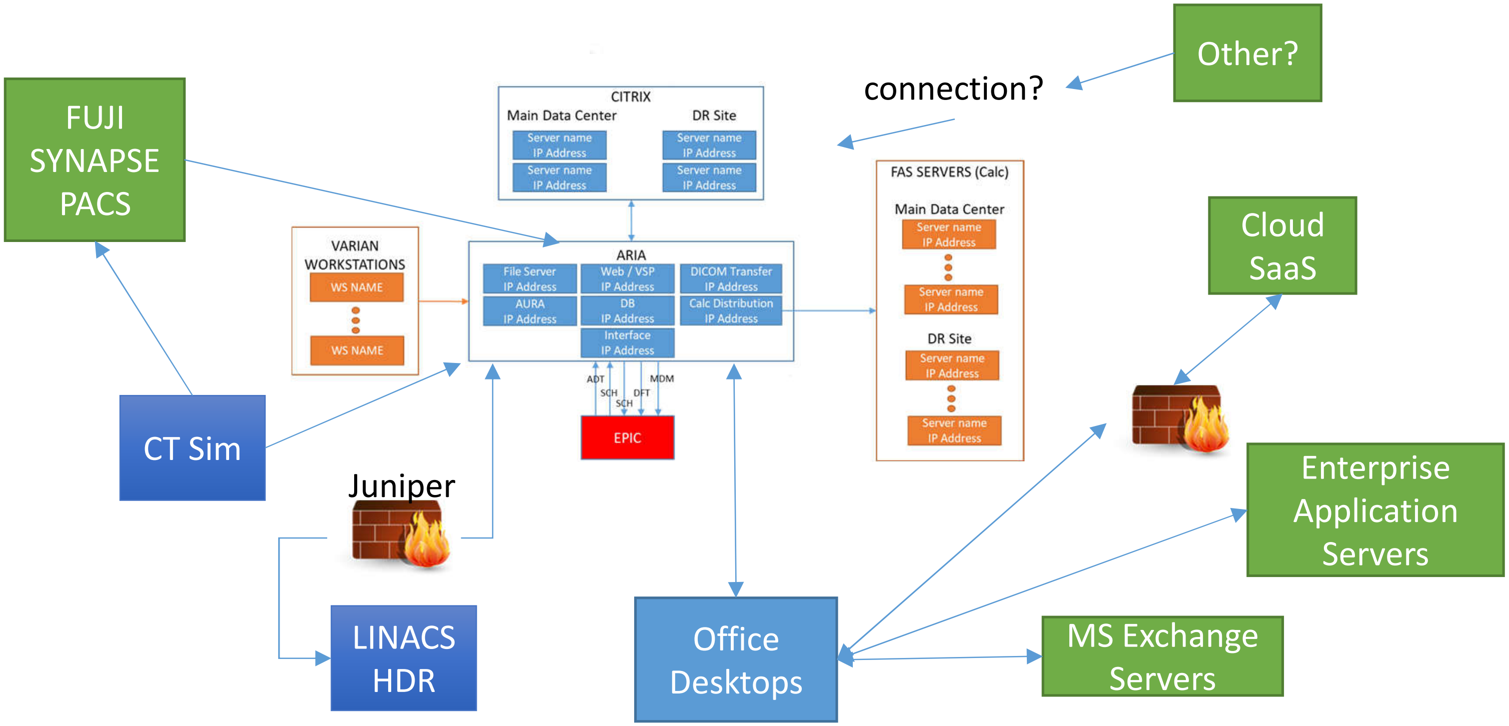
MAPPING: Work with IT to get IP addresses and network routing (arrows).
Know what servers/workstations these applications are installed on.

Server Diagram – Rad Onc



Not shown – Tbox and Archive Servers
Orange: Physical; Blue: Virtual

Information Systems external to department

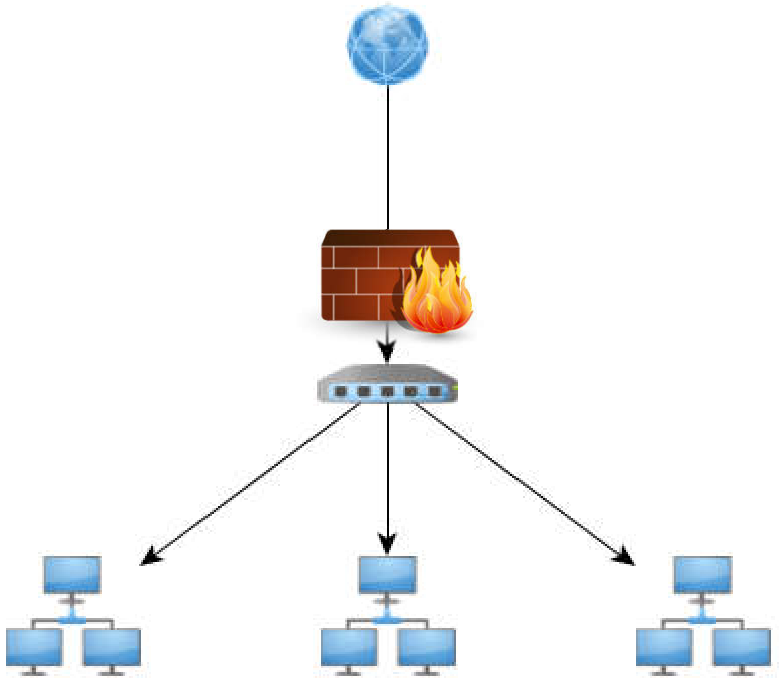


Isolate

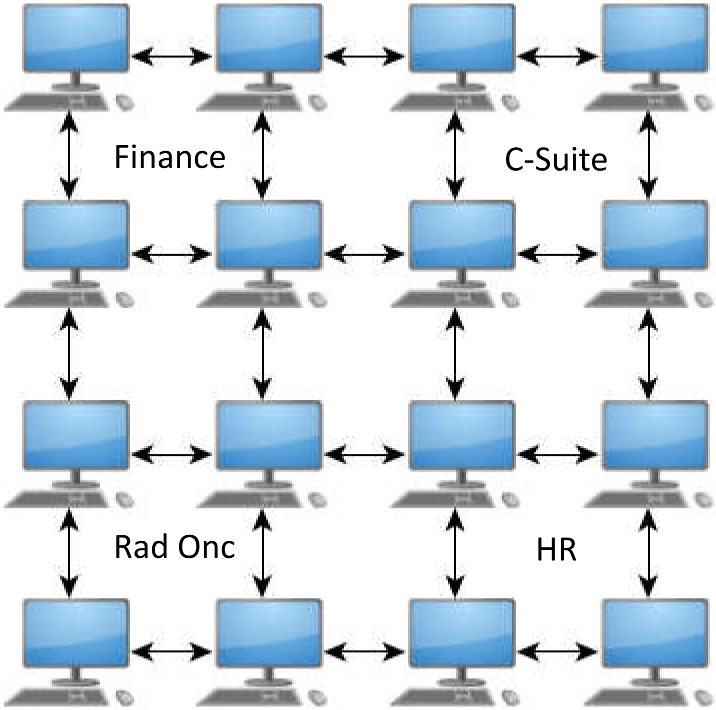
- Determine which devices/systems were affected
  - IT support – run diagnostic tools on systems
- Isolate affected systems/devices from other systems/devices
  - Network Design
    - segregation – air gapping - costly
    - Segmentation*

Segmentation – Firewall and VLAN

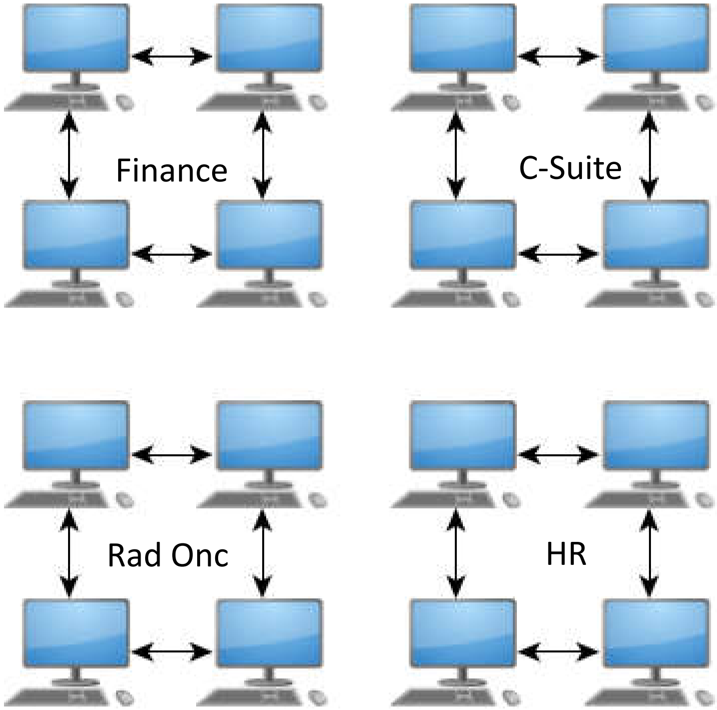
- Firewall
  - keep unwanted traffic out
  - block known sources of malware
- VLAN – group essential related communications on a virtual LAN



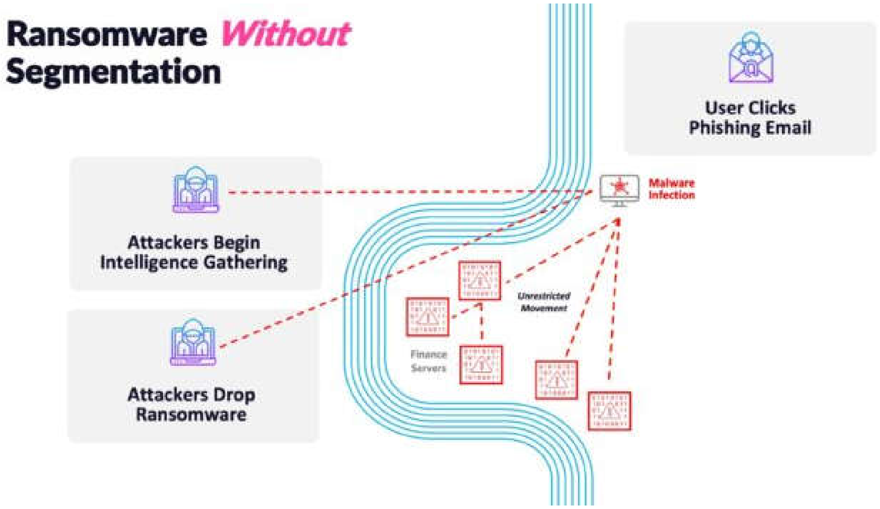
Segmentation Concept



NOT SEGMENTED

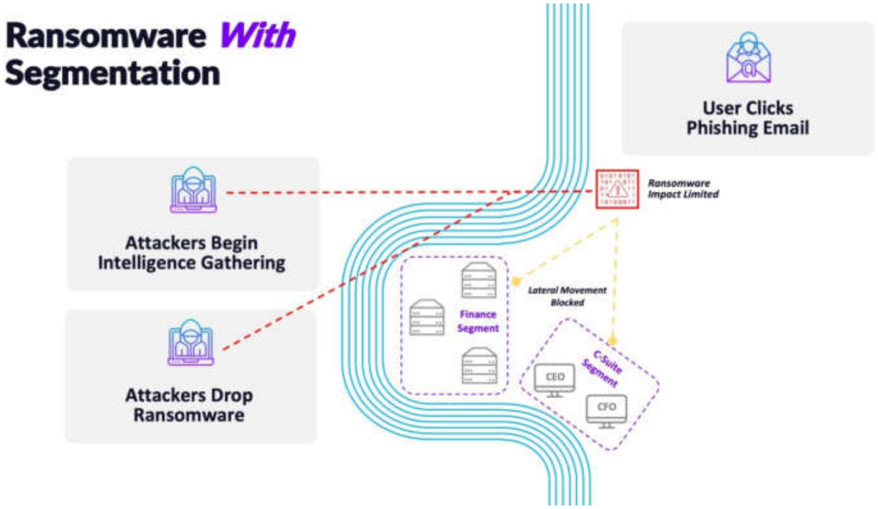


SEGMENTED


Ransomware *Without* Segmentation
User Clicks Phishing Email
Attackers Begin Intelligence Gathering
Malware Infection
Unrestricted Movement
Finance Servers
Attackers Drop Ransomware

Multiple communication paths exist

Communication paths limited to the needed minimum


Ransomware *With* Segmentation
User Clicks Phishing Email
Attackers Begin Intelligence Gathering
Ransomware Impact Limited
Lateral Movement Blocked
Finance Segment
C-Suite Segment
CEO
CFO
Attackers Drop Ransomware

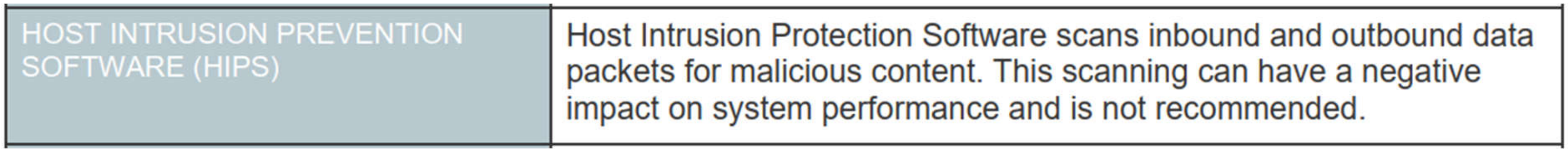
[How Does Ransomware Actually Spread? - Guardicore]

Detect (and respond to) Ransomware ASAP

- Endpoint Detection and Response Software
  - Scan for malware
  - Isolate affected Device
  - Quarantine affected files
  - Stop affected executables
- Application Control
  - Prevent unwanted changes
  - Lock down servers and critical systems

Some Caveats

- Check on CTB-GE-309 (Varian Anti-Virus Software Policy)
  - NO external protection software on computers that are part of the Treatment Delivery System (TDS) – use MICAP instead



HOST INTRUSION PREVENTION SOFTWARE (HIPS)	Host Intrusion Protection Software scans inbound and outbound data packets for malicious content. This scanning can have a negative impact on system performance and is not recommended.

TDS computers rely on timely communications with devices and delays can cause issues with device usage.

Treatment Delivery System – applicable Devices

- 4D Integrated Treatment Console (4DITC)
- On-Board Imaging (OBI) Workstation
- CBCT Reconstruction Computer
- RPM Gating Computer
- In-Room Monitor Workstations
- RPM Workstation
- Acuity Workstation
- CLINAC Console Computer
- Visual Coaching Device (VCD)
- MLC Workstation
- Varian Treatment Workstation
- RGSC Workstation
- BRAVOS Treatment Console
- BRAVOS Service Workstation
- GammaMed iX Treatment Console
- VariSource iX Treatment Console
- Worklist Workstation

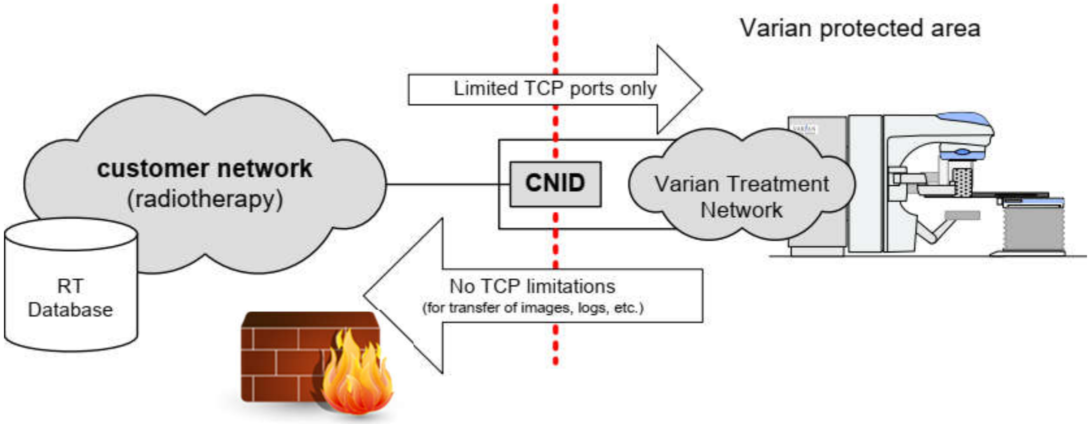
Exclusions

- No real time scanning on certain Folders
  - \Program Files\Varian
  - \Program Files (x86)\Varian
  - \VMSOS
  - VA_DATA$
  - VA_ROOT$
  - DCF$
- No real time scanning on Some directories/ shares for MS SQL
- No Vulnerability testing on Port 57580 of the Eclipse DCF Server

MICAP

- Mission Critical Application Protection
- Secure the Varian Treatment Network (VTN)

CNID = Clinac Network Interface Device = MICAP device (Juniper firewall)



Varian recommends an additional (customer provided) firewall for traffic coming out of the VTN

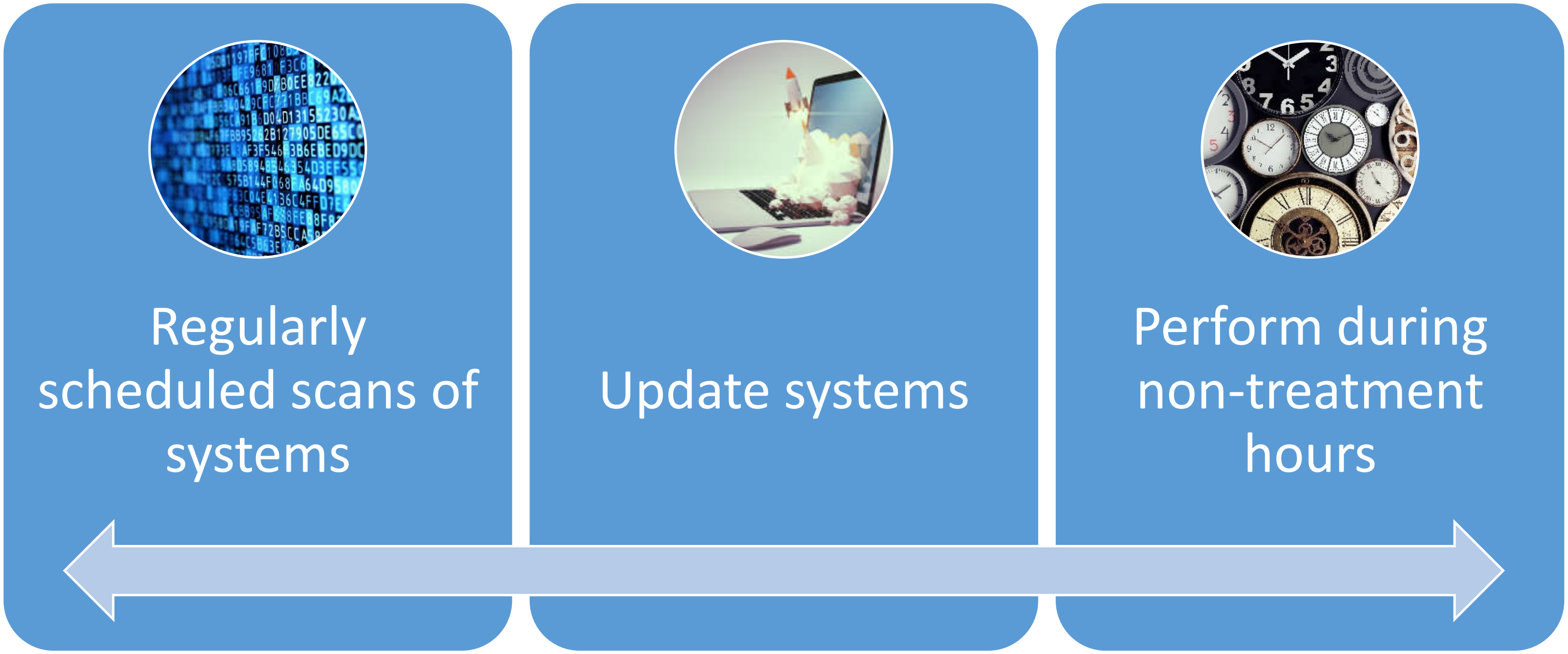
System Hardening

Applications on Workstation

- ⊗ Application 1
- ⊗ Application 2
- ⊗ :
- ⊗ :
- ⊗ Application N

AUTORUN
Mounted Media

Patch Vulnerabilities



Regularly scheduled scans of systems

Update systems

Perform during non-treatment hours

User Response

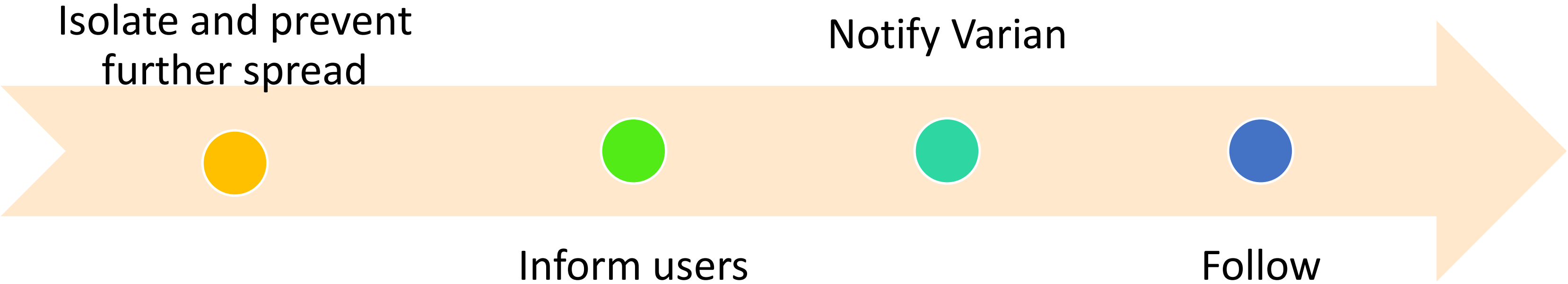
Participate in cybersecurity awareness training

Report suspicious emails to IT

Inform coworkers of the threat

Be careful when looking at spam folders

IT Response



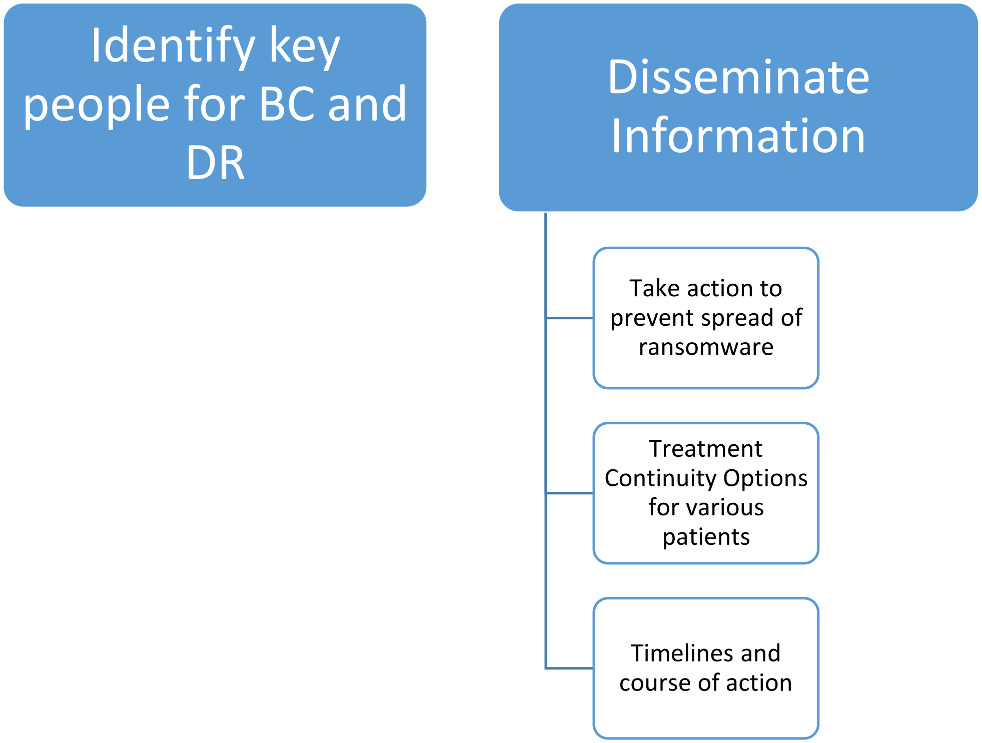
Isolate and prevent further spread

Inform users of the threat

Notify Varian

Follow Business Continuity processes

Respond – Communication plan



Identify key people for BC and DR

Disseminate Information

- Take action to prevent spread of ransomware
- Treatment Continuity Options for various patients
- Timelines and course of action

Backup Systems at WVU

VM snapshot – every 12 hours

- Complete image of the virtual machines at the main center
- Stored at Disaster Recovery site at UHC

Database Replication – every 2 hours

- *ISSUE: document files and images only every 12 hours
- Under discussion for more frequent backup

VM Snapshots

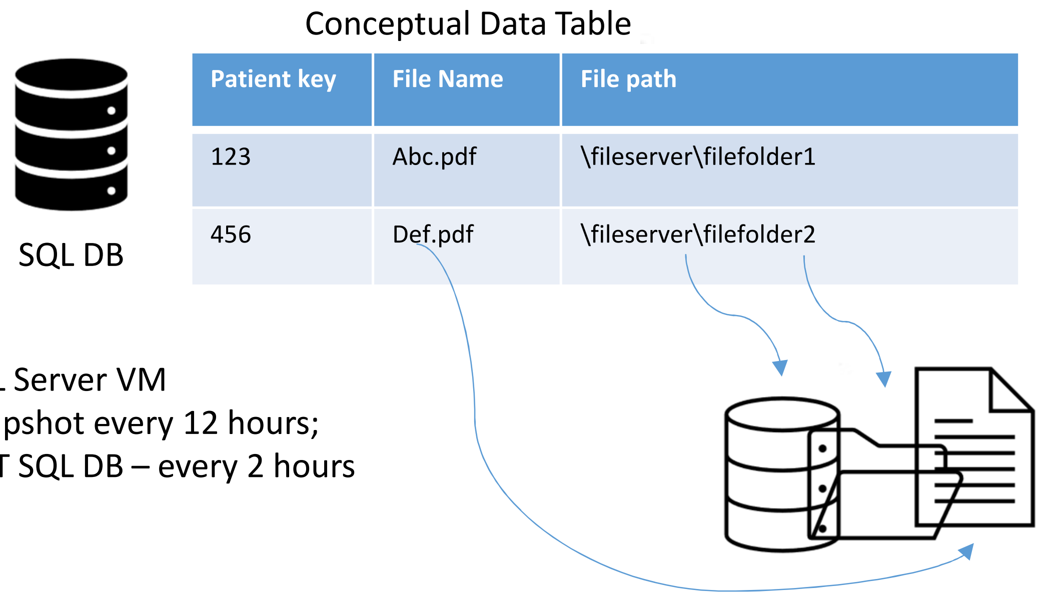
The entire virtual machine is copied.

The copy can be deployed as a virtual machine.

WARNING: RANSOMWARE on the VM will copied also.

- Ensure the VM Snapshots are clean before deployment
- May need to use an earlier VM Snapshot, more data loss possibly

Aria – where is the data? What’s the problem?



Conceptual Data Table

Patient key	File Name	File path
123	Abc.pdf	\fileserver\filefolder1
456	Def.pdf	\fileserver\filefolder2

SQL DB

SQL Server VM
Snapshot every 12 hours;
BUT SQL DB – every 2 hours

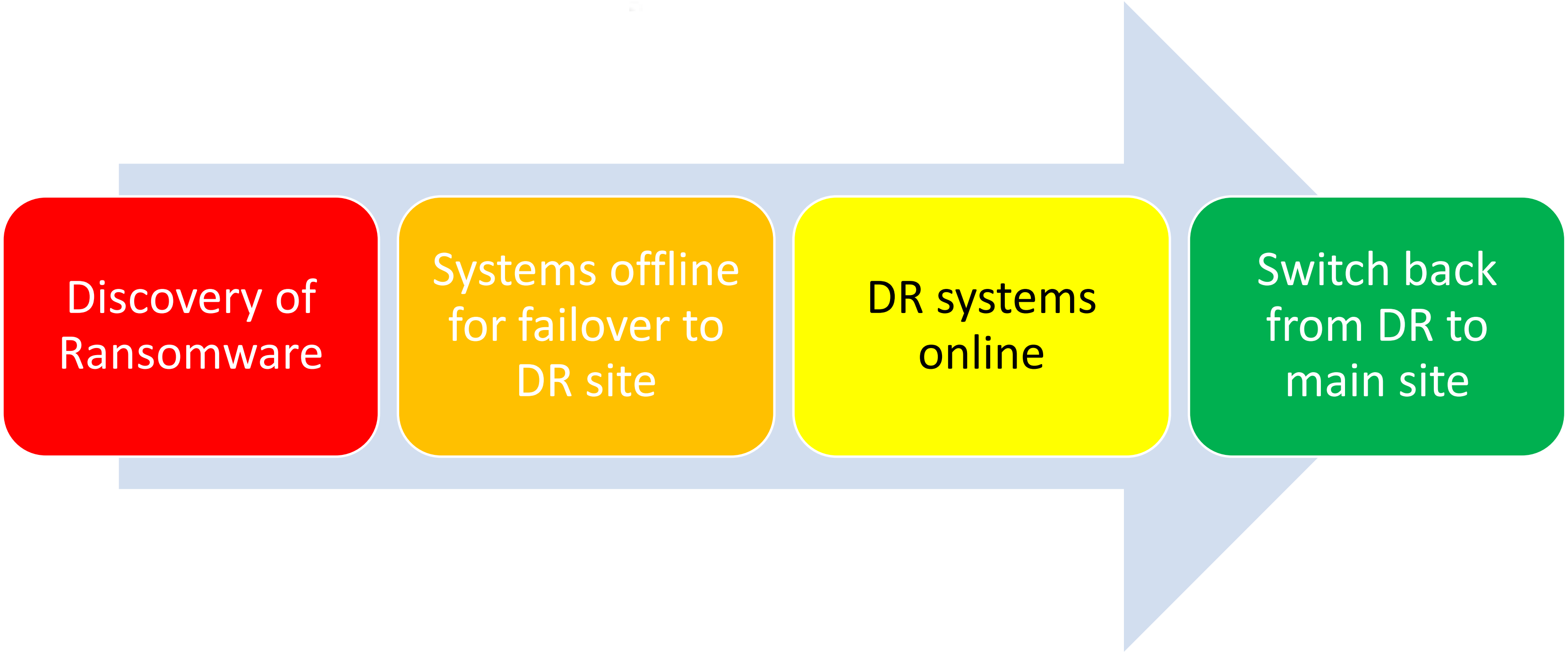
File server – on a VM, snapshot every 12 hours

Possible Failure Scenario

Time	User Action	Main SQL	Main File Server	SQL Replica	File Server VM snapshot
6 PM		Scheduled replication	Scheduled snapshot	updated	updated
7 PM	Add Document	Document Path added	Document added	No update yet, document path missing	No update, document missing
8 PM		Scheduled replication		Updated and has document path	No update, document missing
9 PM		DISASTER – unavailable	DISASTER – unavailable	Has document path	Document missing
11 PM		Offline	Offline	Put into production	Put into production
11:30 PM	Access Document	Offline	Offline	Document path referenced	UNABLE TO PROVIDE DOCUMENT – PATH DOES NOT EXIST
11:45 PM	CALLS IT in a panic!	Offline	Offline	??? Crashed????	???Crashed???

LESSON LEARNED: SYNCHRONIZE THE SQL DB REPLICA AND THE FILE SERVER VM SNAPSHOT

RANSOMWARE BC stages



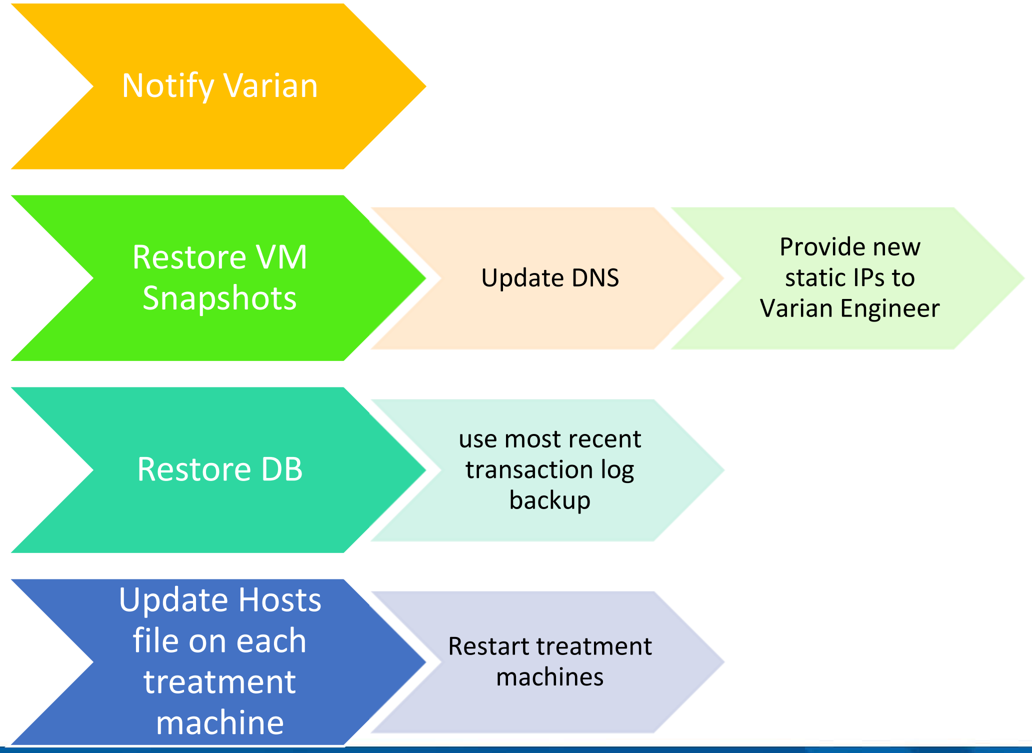
Discovery of Ransomware

Systems offline for failover to DR site

DR systems online

Switch back from DR to main site

Disaster Recovery workflow



Notify Varian

Restore VM Snapshots → Update DNS → Provide new static IPs to Varian Engineer

Restore DB → use most recent transaction log backup

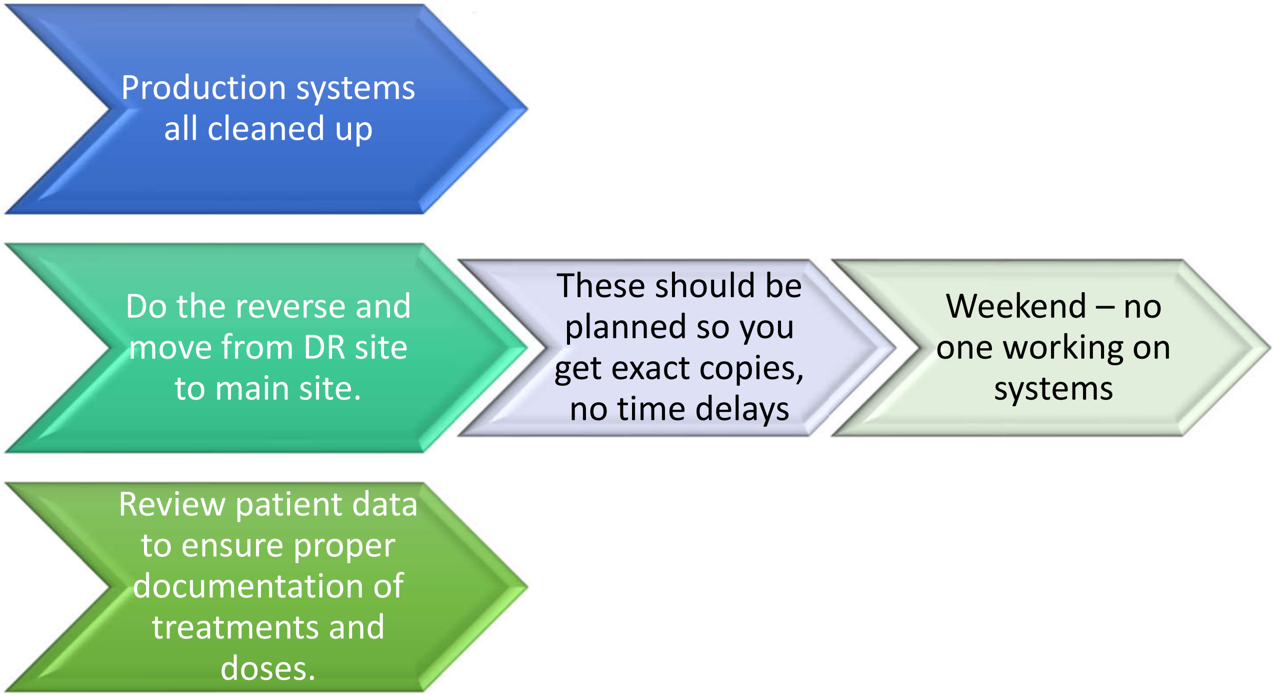
Update Hosts file on each treatment machine → Restart treatment machines

After DR site is up

Transfer any manually recorded items for treatments done offline

Reconcile patient charts

Switching back after DR



Production systems all cleaned up

Do the reverse and move from DR site to main site.

These should be planned so you get exact copies, no time delays

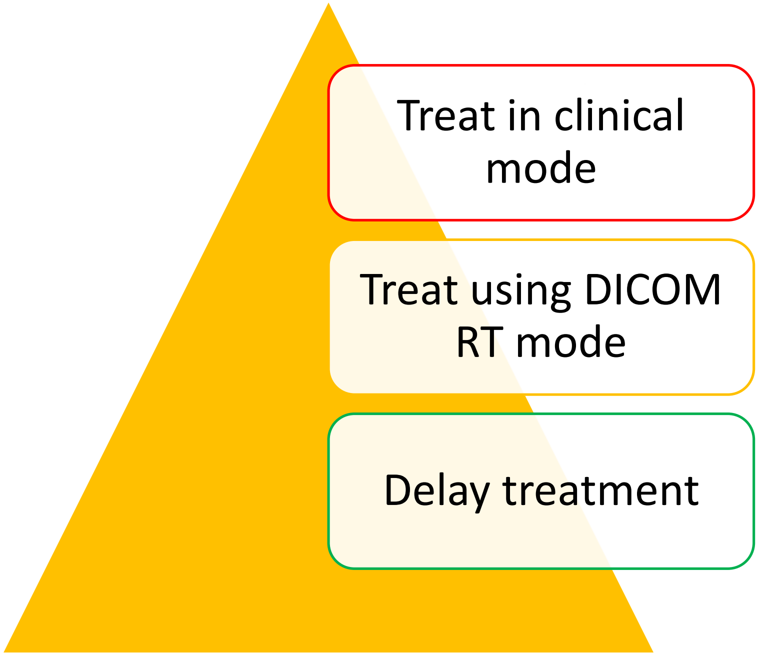
Weekend – no one working on systems

Review patient data to ensure proper documentation of treatments and doses.

TIMING QUESTIONS

- Earliest Time to recovery = 3 hours
- Over what time was data lost?
- How much data was lost?

Business Continuity Options during Failover Process



Treat in clinical mode

Treat using DICOM RT mode

Delay treatment

Triage patients

Which patients can wait until services are restored?

Which patients can't afford any interruption?

- Clinical Setups
- DICOM RT Mode

Clinical Setups

- Simple plans - Hand Calcs - Paper Chart
- C-Series: Clinical Mode
- Truebeam:
  - Unplanned Treatments ? No.
  - Service Mode? Pretty bad idea…
  - Prepare plans and use File Mode?
    - ad hoc tools to create plans?
    - standard whole brain, SVC, etc plans?
  - Just don’t do emergencies?
  - Discuss…

What if this can’t be fixed right away?

Certain patients can’t be delayed for too long

DICOM RT MODE possibility

Have to consider additional patients at time of treatment planning

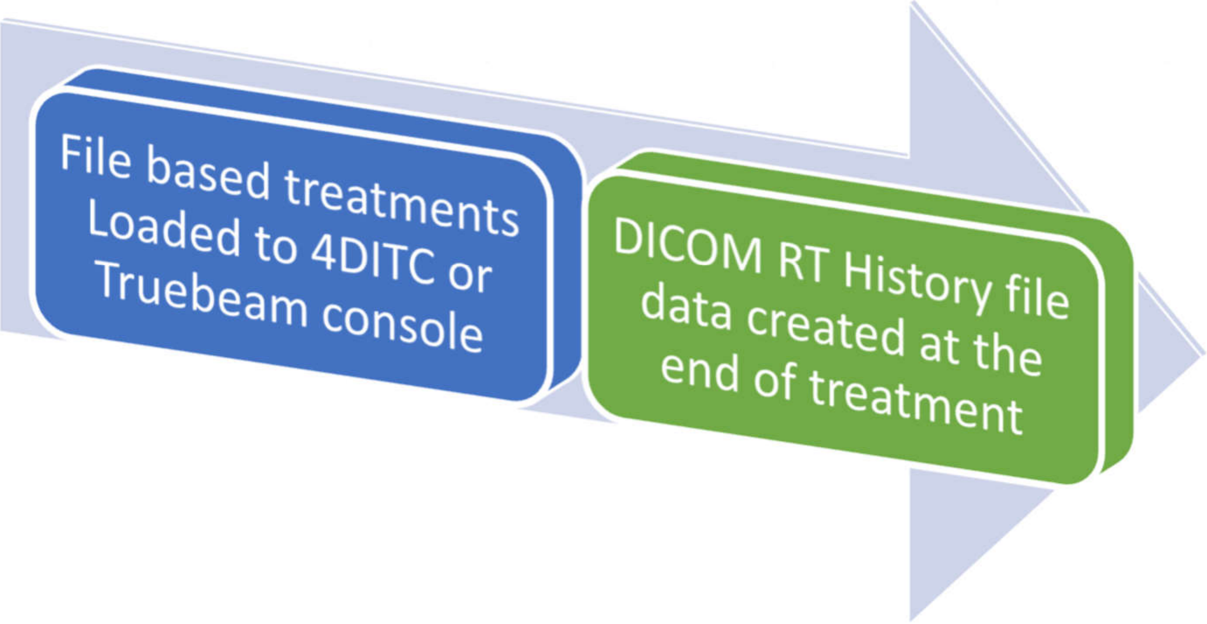
- PART OF BC for other scenarios, eg, Fire, Flood.

Treatment Scenarios By Timeline

	Clinical Treatments	DICOM-RT
Day 0 – machine goes down	Whole brain, spine, SVC - emergencies	
Day 1	Emergencies; plan to transfer emergencies to another clinic	
Day 2	Transfer emergencies	Critical patients – aggressive disease – some lung case, head and neck
Day 3	Transfer Emergencies	Critical patients

NOTE – this is only conceptual. Work with your physicians to come up with a process.

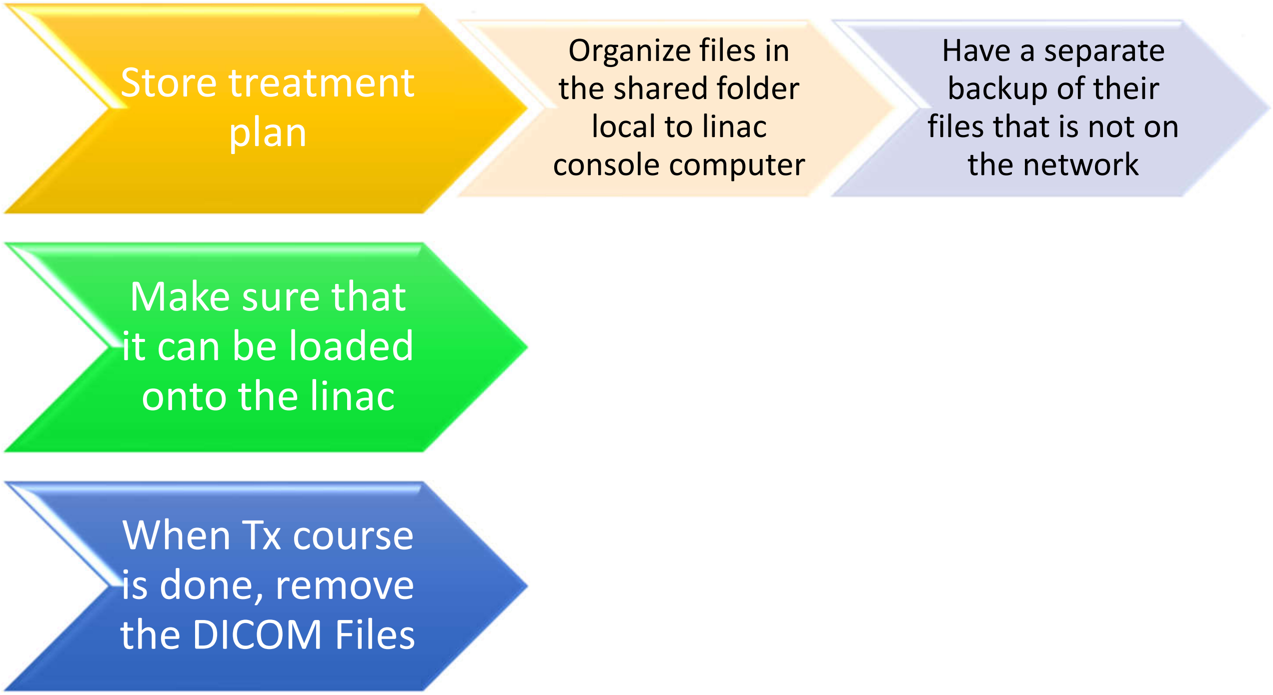
DICOM RT Mode



File based treatments Loaded to 4DITC or Truebeam console

DICOM RT History file data created at the end of treatment

DICOM FILE MODE Management



Store treatment plan

Organize files in the shared folder local to linac console computer

Have a separate backup of their files that is not on the network

Make sure that it can be loaded onto the linac

When Tx course is done, remove the DICOM Files

DICOM objects to export in preparation for file mode

RT plan, including setup fields

- RP.xxxxxx.dcm
- *

RT reference images (if applicable)

- RT Image : RI.xxxxxx.dcm

Treatment plan CT:

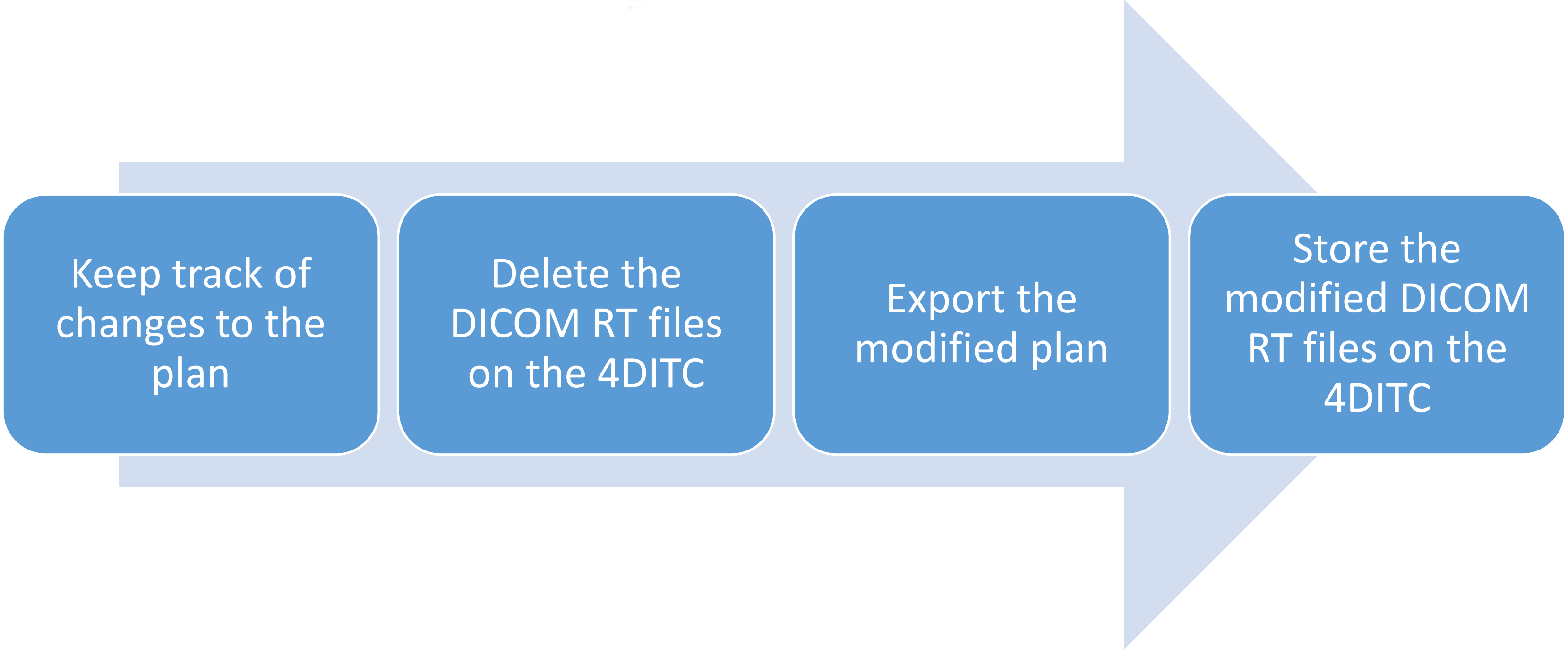
- CT. xxxxxx. dcm

RT structures for localization

- RS.xxxxxx.dcm

*E.g., RP.1.2.246.352.71.5.413.484.20051018160201.dcm

If plan changes:



Keep track of changes to the plan

Delete the DICOM RT files on the 4DITC

Export the modified plan

Store the modified DICOM RT files on the 4DITC

BE CAREFUL DURING TREATMENT

MAKE SURE YOU ARE LOADING THE CORRECT PLAN FOR THE CORRECT PATIENT

IT IS CRUCIAL TO ORGANIZE THE FILES PROPERLY TO PREVENT THIS CONFUSION

The normal failsafe features of ARIA are not available

DICOM objects to import after treatments

RT Treatment History	• *RT.xxxxx.dcm
Acquired Images	• RT Image, RI.xxxxx.dcm
RT Spatial Registration	• RE.xxxxx.dcm

*Use a naming convention for the history files –
Example – include the Fraction number, date, patient ID in the file name

Stay Up to Date

Work with Varian Service Engineer, Applications Trainers

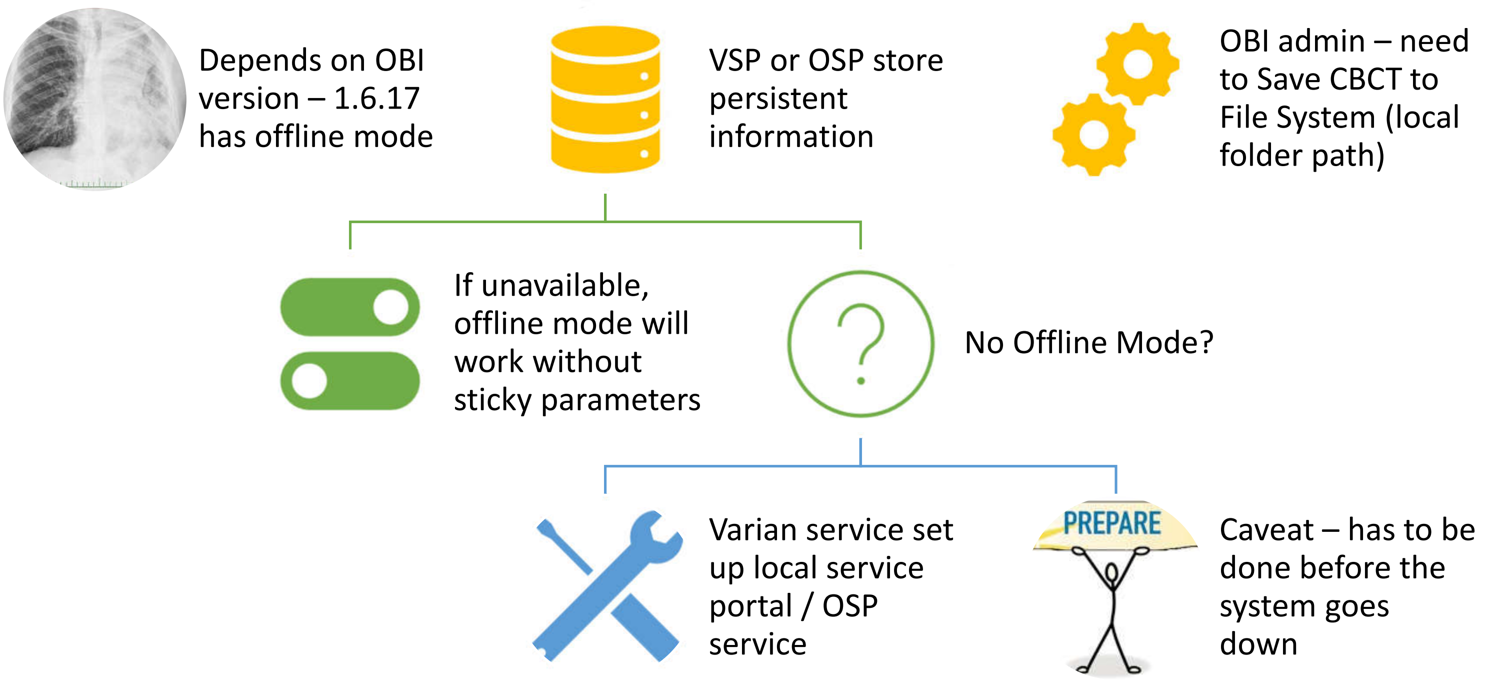
- Functionality specific to your platform and version

Clinical Mode or Unplanned Treatment Mode

DICOM RT mode

OBI, Imaging

Prepare for Imaging – C Series



Depends on OBI version – 1.6.17 has offline mode

VSP or OSP store persistent information

OBI admin – need to Save CBCT to File System (local folder path)

If unavailable, offline mode will work without sticky parameters

No Offline Mode?

Varian service set up local service portal / OSP service

Caveat – has to be done before the system goes down

Truebeam Caveats

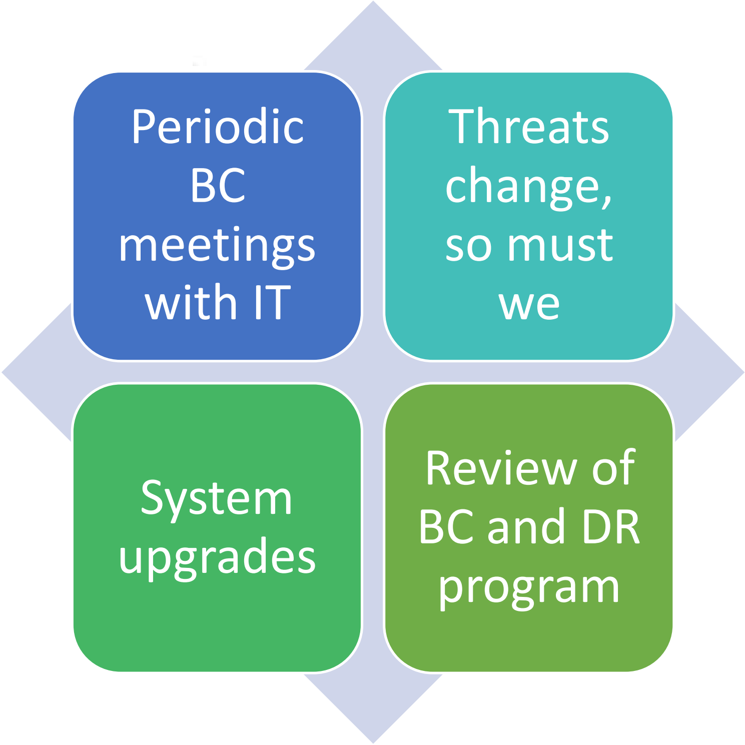
If Aria is down but VSP is up, use File Mode.

Officially – if VSP is down, Truebeam is down.

Unofficially, if ARIA, VSP, and AD are down, you could install a local VSP and treat with a generic username and password.

- This is very involved – consider solution only if more than 3 days down.
- For File MODE only
- Can't treat emergency cases (no plan available)

Continuous Improvement



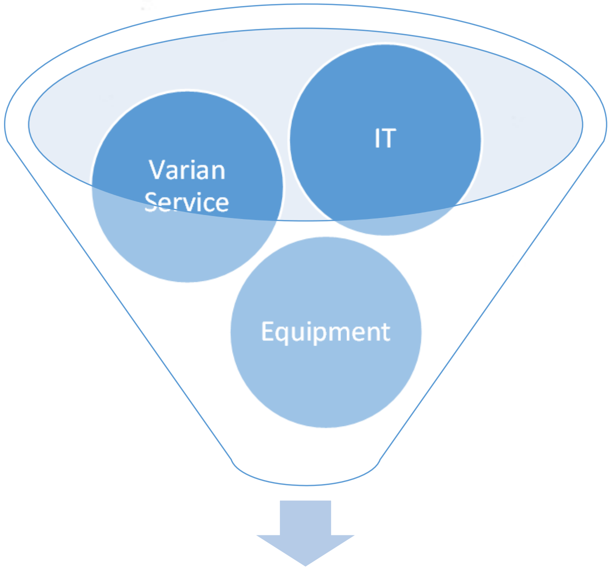
Periodic BC meetings with IT

Threats change, so must we

System upgrades

Review of BC and DR program

Collaborate



BC plan specific to your environment

Conclusion

- Plan for a ransomware event
  - Prevent – Segmentation, Anti-Virus, cybersecurity training
  - Prepare – Manual Treatments, File Mode, clinical workflows, Failover workflow
    - Know all your systems and how they are connected
    - Test the workflows
  - Respond – implement failover and clinical protocols

References

1. Sophos:
   a) The State of Ransomware 2022
   b) The State of Ransomware 2021
2. National Institute of Standards and Technology (NIST) publications:
   a) Ransomware Risk Management: a Cybersecurity Framework Profile NIST.IR.8374
   b) Guide for Conducting Risk Assessments. Nist special publication 800-30 r1
3. Varian documents:
   a) Backup Guidelines. CTB GE-936.
   b) Disaster Recovery (DR) User Implementation Reference Guide. UG-GE-DRRG-A
   c) Mission Critical Application Protection (MICAP) Whitepaper. CTB MI-781
   d) Recommendations on Securing Customer Purchased Varian Products from Ransomware. CTB GE-1076.
   e) Anti-Virus Software Policy. CTB GE-309-Q
   f) DICOM RT Mode Reference Guide P1048021-001-A
   g) TrueBeam Instructions for Use P1033680-002-B