Cybersecurity and the Medical Dosimetrist

Marc Mlyn, MS, MBA, CMD

1

Agenda

Setting the Stage

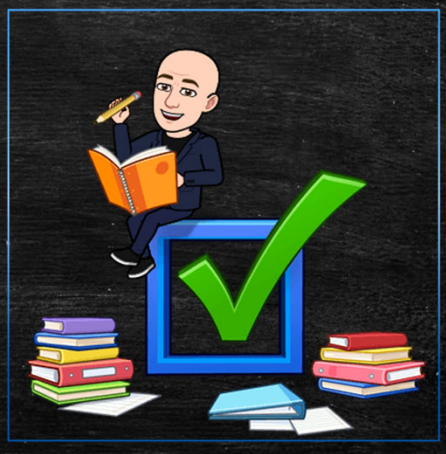
- About the presenter
- Goals of this presentation
- What is TG393

Cybersecurity

- Cyber-events – how/what/why
- Trends

Radiation Oncology

- Assessing operations / risk
- Where does the CMD fit in?



2

Agenda

Contingency Planning

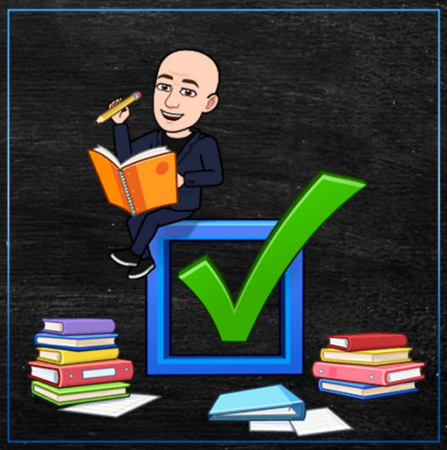
- What is a contingency plan
- Triage & risk management
- NIST

Take Aways

- What you should do next
- Tips and tricks

Challenges and the Future

- Challenges in the hospital
- Future of our industry and cyber



3

Disclosures

1. Quantum Financial Interest: The presenter has a financial interest in Schrodinger's Cat Corporation. The company is currently both bankrupt and highly profitable until an auditor opens the books.2. Dietary Funding: This research was fully funded by the local donut shop. As a result, all data points shaped like circles are legally obligated to be referred to as "sprinkle-friendly zones."
2. Dietary Funding: This research was fully funded by the local donut shop. As a result, all data points shaped like circles are legally obligated to be referred to as "sprinkle-friendly zones."
3. Mathematical Incompetence: The author confesses that the complex calculus on Slide 14 was actually derived by their smart fridge, which is currently running a more stable operating system than their laptop.
4. Timeline Collision: The presenter cannot rule out the possibility that a future version of themselves traveled back in time to mess up the error bars on Graph 3.
5. Corporate Sponsorship: The laws of thermodynamics discussed in this presentation are brought to you by Red Bull. Red Bull: Attempting to violate the conservation of energy since 1987.
6. AI Assistance: The hypotheses in this paper were generated by an AI chatbot that was explicitly told to pretend it was a Victorian-era physicist who had drank too much espresso.
7. Wardrobe Malfunction: The tweed jacket being worn by the speaker has not been dry-cleaned since the pre-pandemic era, creating an localized ecosystem that may skew the room's ambient humidity data.

4

5

Disclosures

Just kidding… don't you hate when presenters fly by their disclosures?

6

About the presenter

Marc Mlyn (CMD since 1994)

- I am President and CEO of RaySearch Americas but will not wear this hat today
- I am on the ASTRO Corporate Advisory Board
- I am on the AAPM Corporate Advisory Board
- I am a director on the board of the Medical Physics Institute (MPI)

In industry since 1997 (Philips & CIVCO)

- I am on the planning committee for IHE-RO
- MBA (2005) and MS in Cybersecurity (2024)
- I am a member of TG 393 – because cyber risk is a call to action…
- I was the first AAMD "webmaster" in 1997!

7

Goals of this presentation

- Understand cyber threats and how they manifest in radiation oncology
- Understand how contingency planning can help keep patients safe – and how you fit in
- Understand the purpose of TG393
- Come away with specific knowledge that you can apply back home
- Not make you all fall asleep

Nothing is more terrible than ignorance in action.

Johann Wolfgang von Goethe

8

On-line Survey

Please complete this survey during the presentation!

We will publish the results online.

IMPORTANT: Please only submit one survey per Radiation Oncology Department

9

AAPM TG-393

The charges support the implementation of contingency plan for a radiation therapy clinic to resume patient treatments within a reasonable timeframe, following a cyberattack that leaves institutional computing and network services compromised and/or unavailable.

1. Provide guidance in analyzing each clinical sub-system's weaknesses and specifying clinical priority or impact of each clinical sub-system.
2. Provide recommendations and perspective to review and to determine the readiness of the clinical systems against cyberattacks and to prepare for readiness of contingency plan for each clinical subsystem.
3. Identify the nature and the severity of attacks and provide the minimum dataset to be prepared and recommendations on appropriate time period (hours or days) to recover from the attack per the levels of the attacks.
4. Provide the data backup strategies for contingency plan of each clinical subsystem.

10

AAPM TG-393

5. Provide recommendations and strategy in rebuilding temporary clinical systems in case of cyberattacks and using the temporarily-rebuilt subsystems to resume radiotherapy treatment.
6. Provide guidance and strategy to verify corrupted clinical system and to recover corrupted clinical data.
7. Provide recommendations on how to restore patient data back to the main clinical system after restoration of institutional computation and network services.
8. Provide guidance to individual clinical practices in designing their own site-specific contingency plan from minimal to comprehensive.

11

Current Status of TG-393

- Initial report is completed and has been reviewed by various committees in AAPM.
- Minor and major comments are currently under review.
- The primary issues revolve around how specific we can get with recommendations.
- Should be completed by the end of the year.

12

What happens after TG-393 is released?

- AAPM / EFOMP / OTHER website for current information
- Annual survey
- Conference presentations
- Enhanced vendor coordination (ASTRO and AAPM CAB, extended work with RTSEC and IHE-RO, etc.)
- Periodic report updates
- Standing cybersec committee in AAPM (?)

13

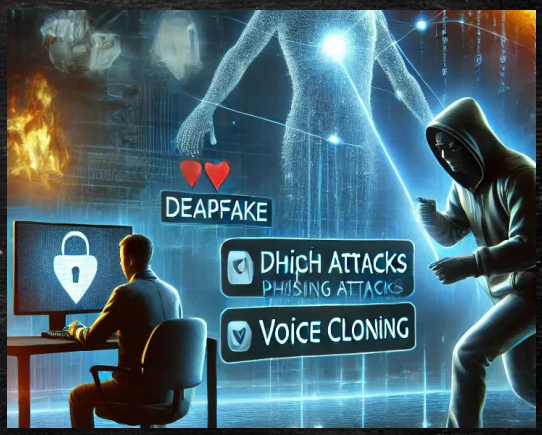
Cybersecurity Threats in 2026

- AI-Powered Phishing & Social Engineering
- Ransomware & Double/Triple Extortion
- Identity & Credential-Based Attacks
- Supply Chain & Third-Par… on…
- Zero-Day Vulnerability Exp…
- Deepfake & Synthetic Ident… Fr… c…
- Data Breach & DDoS Attacks
- Cloud Misconfiguration Exploits
- Critical Infrastructure Targeting
- AI-Autonomous Malware & Agentic …cks
- …on-State Espionage & Geopolitical …acks
- …nsider Risk in Hybrid Work Environments
- …oT & Edge Device Exposure

14

AI-Powered Phishing & Social Engineering

- AI enables attackers to scale social engineering by generating realistic messages, voices, and personas. This reduces traditional red flags and increases the success rate of phishing and impersonation attacks.



15

Ransomware & Double/Triple Extortion

- Modern ransomware attacks often involve encrypting data, stealing it, and threatening public exposure. Triple extortion adds pressure by targeting customers or partners of the victim.

16

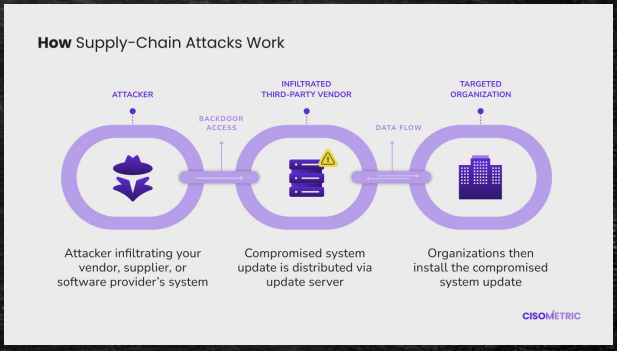
Identity & Credential-Based Attacks

- Credential theft enables attackers to bypass perimeter defenses and impersonate legitimate users, often leading to deeper compromise.
- Credential "stuffing" is when cyber criminals "try" IDs and passwords they have purchased on the dark web.

17

Supply Chain & Third-Party Compromise

- Supply chain attacks compromise trusted vendors or software components, allowing attackers to infiltrate multiple downstream organizations.



18

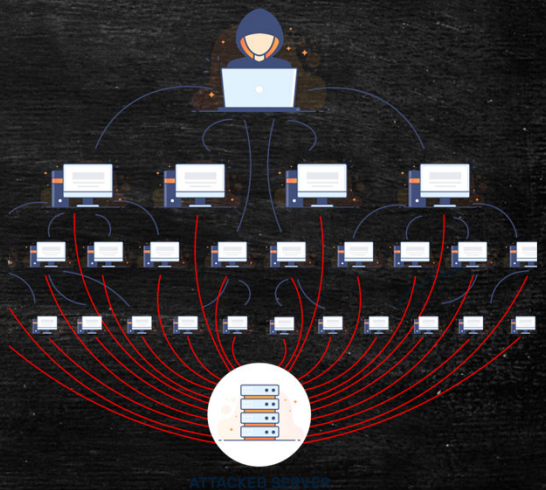
Zero-Day Vulnerability Exploitation

- Zero-day exploits target vulnerabilities unknown to vendors, giving attackers a window of opportunity before patches are available.

19

DDoS Attacks

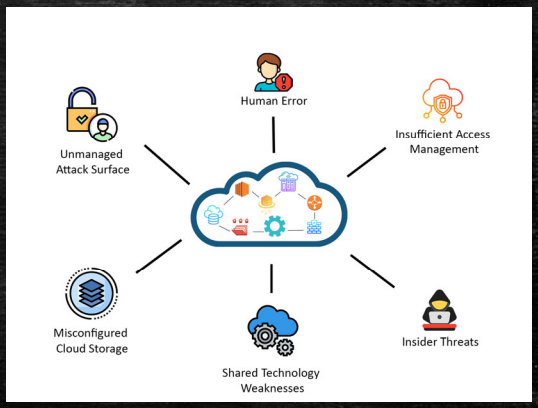
- DDoS attacks overwhelm systems via controlled botnets, causing outages and operational disruption.



20

Cloud Misconfiguration Exploits

- Cloud misconfigurations occur when security settings—like public access, identity roles, or network rules—are improperly configured. Attackers scan the internet for exposed cloud assets and exploit them to steal data or gain footholds.



21

Critical Infrastructure Targeting

- Critical infrastructure—energy, water, transportation, healthcare—is increasingly targeted because disruptions have high impact. Attackers often aim for extortion, espionage, or geopolitical leverage.

22

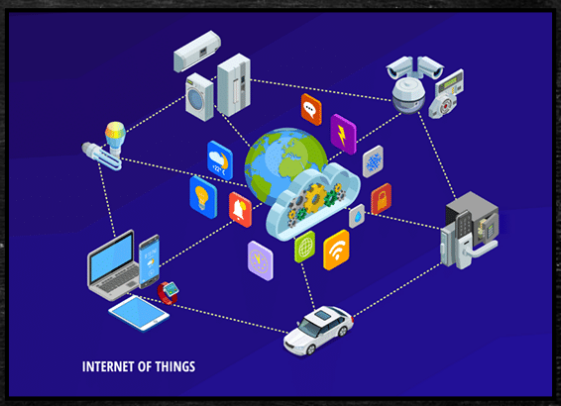
Insider Risk in Hybrid Work Environments

- Insider risks include malicious insiders (theft, sabotage) and unintentional insiders (mistakes, negligence). Hybrid work environments expand the attack surface with more devices, networks, and unmanaged tools.

23

IoT & Edge Device Exposure

- IoT and edge devices often lack strong security controls and are deployed at scale. Attackers exploit weak authentication, unpatched firmware, and exposed services to gain access or build botnets.



24

Glossary of Terms

- APT – Advanced persistent threat
- DDoS – Distributed denial of service
- CIA – Confidentiality, Integrity, Availability
- IAM – Identity and access management
- Vulnerability – Weakness in a system
- DR and HA – Disaster recovery and High Availability
- Defense in Depth – more than one level of security safe guards
- RTO / RPO – Return to operations, recovery point objective
- Data exfiltration – Data has been downloaded by the bad guys

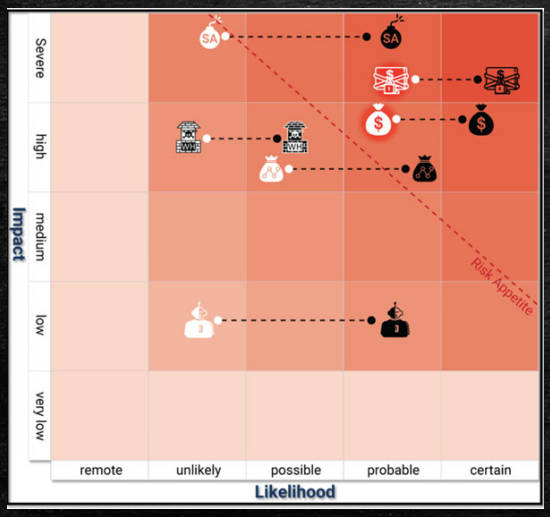
25

Glossary of Terms

- Incremental vs Differential
- Least privilege access
- MAC address – equipment specific identifier
- MIM – Man in the middle attack
- NAT – network address translation
- IDS – intrusion detection system
- Non-repudiation – ability to assign responsibility for an action
- Blue team and red team – defense and offense testers
- Network segmentation – separating parts of a network to isolate devices
- Smishing – SMS + phishing
- CVE – Common vulnerabilities and exposures - https://www.cve.org/

26

Understanding Risk Mitigation



- SA – Sabotage (DDoS, Wiper Malware, Data Blackmail)
- EX/FF – Extortion and Financial Fraud (Ransomware, ACH fraud, payment data theft)
- DT – Data Theft (PHI, customer data)
- RH – Resource Hijacking (botnet, CPU/GPU cycle usage, etc.)

Risk is never fully mitigated!

27

Weak Points in Radiation Oncology

- People (phishing, social engineering, bad cyber hygiene at the user level)
- Lack of frameworks and regular discipline in hospital IT organizations
- Lack of management direction on risk appetite
- Lack of contingency plans to minimize poor RTO (return to operations – how quickly) and RPO (recovery point objective – how much are you willing to lose) – *specific* to Radiation Oncology
- Rebuilding and return to full operation can take weeks to months

28

HHS Performance Goals (Essential)

1. Mitigate known vulnerabilities
2. Email security
3. Multifactor authentication
4. Basic cybersecurity training
5. Strong encryption
6. Revoke credentials from departing users
7. Basic incident planning and preparedness
8. Unique credentials
9. Separate user and privileged accounts
10. Vendor / supplier cybersecurity requirements

29

HHS Performance Goals (Enhanced)

1. Asset inventory*
2. 3rd party vulnerability disclosure*
3. 3rd party incident reporting
4. Cybersecurity testing*
6. Detection and response to TTP's (tactics, techniques and procedures)
7. Network segmentation*
8. Centralized log collection*
9. Centralized incident planning and preparedness*
10. Configuration management

30

Radiation Oncology Subsystems

- Assess at two levels
- First is system type, and then classify aspects of each system:

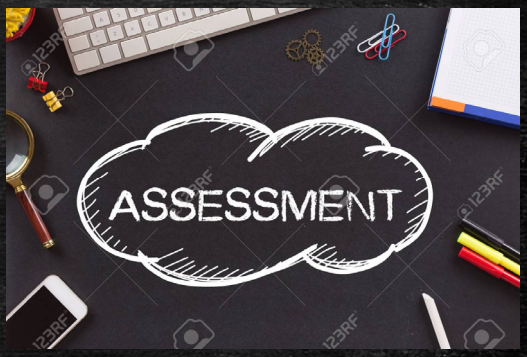
Hardware

Software

Data

Interconnectivity

Importance



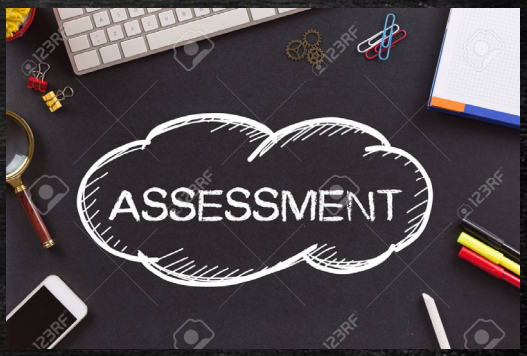
31

Radiation Oncology Subsystems

Hardware – how unique is the HW? Where is it? Can we store copies in case?

Software – do we have have backup copies? Can we install it ourselves? Where does it get installed?

Data – what kind of data is it? Where is it stored? Is it easy to see if it is corrupted?

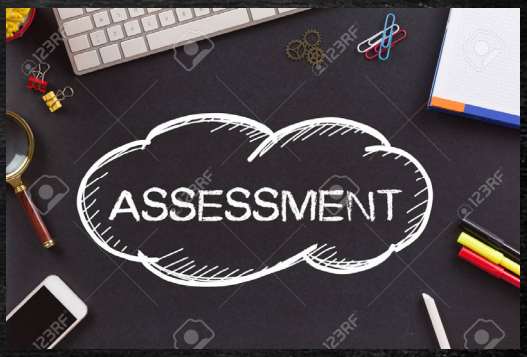


32

Radiation Oncology Subsystems

Interconnectivity – how important is the network to the functionality? Can the data be moved manually? Is the internet needed?

Importance – how important is the data? Do we need all historic data, or is it ok to start fresh? Can patients be treated safely without it?



33

More than just Radiation Oncology Tools

- Admin systems (HIS, other hospital registrations tools)
- Central IT services (email, AD, remote access, phone)
- Hospital / Dept. Imaging
- OIS
- TPS
- QA
- Ancillary software (QA, daily and summation, billing sw)
- Tx delivery systems (linacs, etc)
- In room imaging systems
- Positioning / Immobilizatiom

34

What if the worst comes to pass?

- Can the front desk communicate with patients or with staff?
- Can the linac operate offline?
- How will you deliver plans? This is not the old days with simple fields.
- What processes are ok to "skip" during an emergency?
- What is safe vs unsafe? Balancing risk…

35

Who should be involved?

- Radiation oncology needs an "incident response team"
- See AAPM working group on cybersecurity (report 438) – Stakeholders
- Everyone should be represented – with strong technical leadership
- Responsible for cyber assessment and response

36

Cybersecurity Responsibilities – WGCS

Medical Physicists / CMD's

- Technology selection and prevention
- Understand infrastructure, connectivity, assist with asset management
- Admin / preparation – downtime manual
- Onsite support during an event
- Assure treatments are recorded
- Caution not to extend infection while using media
- Recovery strategies – bridge gap between HIT and MD's
- QA on recovery
- Reconcile / reconstruct patient chart and plans

37

Let's talk about us

- The dosimetrists and therapists are most knowledgeable about patient plans and status
- The dosimetrists know the TPS better, while the therapists tend to know the OIS better
- You need to ask the question – is this data backed up? What happens if the systems crash tomorrow?
- When patients are treated during an outage, the CMDs and RTTs need to understand what they will be doing and why.

38

Things to consider as the CMD

- Understand the backup strategies – YOU will need to replan what is not there
- Insist on testing whatever planning or OIS system will be implemented during the event
- Investigate what your TPS can do to help – backup planning, machine learning, import backup files, dose accumulation, etc.
- Take an active role in assessing how patients will be treated on the linac (service mode, etc.).
- Take an active role in assessing how new / modified plans will be used to reconcile existing plans (accumulated dose, etc.)
- Work with physics to assess QA (need, process, documentation)

39

Preparation

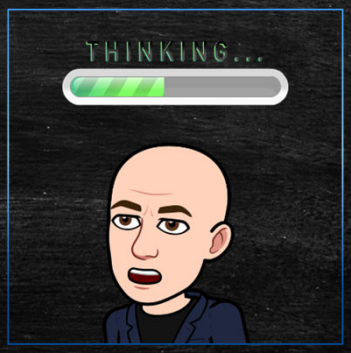
- Make sure you are a part of the plan. Ask to be involved!
- Don't be afraid to say, "what about…?"
- Backup plans or data from a month ago is not going to help you much.
- Utilize features in the TPS to minimize work if the worst comes to pass (e.g. Fallback planning or other tricks).
- Drill, Drill, Drill!

- Work with vendors to make sure they are part of the contingency plan!

40

Regarding Contingency Plans

- You cannot have a contingency plan in a vacuum.
- Any "plans" need to be coordinated with the hospital.
- You could have more than one plan (short term, med term, etc.)
- Goals need to be defined – how you will operate and how / when you will treat patients.
- Plans need to be immediately implemented!



41

Regarding Contingency Plans

- You cannot have a contingency plan in a vacuum.
- Any "plans" need to be coordinated with the hospital.
- You could have more than one plan (short term, med term, etc.)
- Goals need to be defined – how you will operate and how / when you will treat patients.
- Plans need to be immediately implemented!
- What is the difference between a business continuity plan and a contingency plan?

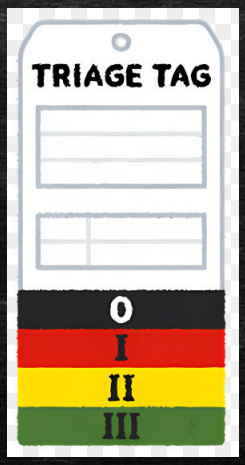
BC plan purpose puts financial / operational goals in front.

CP purpose is the technical plan that will enable you to treat patients.

42

The Importance of Triage

- There are so many systems, patient types, financial and political issues, etc., that triage becomes critical.
- Some major institutions triage on patient intake, so decisions need not be made on the fly later.
- Defines at what "stage" of system / department recovery a patient can be treated.



43

Core Concepts of a Plan

- Admin will generate patient contact info.
- Employees will use cell phones to communicate.
- Vendors have provided backup hardware to be stored in a closet – temp installations within 24 hours.
- Backups will be daily incremental, weekly differential.
- Linac treatments will be performed in service mode.
- New patients will not be started unless triage level I.
- All staff will be onsite, except for a subset so internet can be utilized.
- iRT will be in constant communication with hospital central admin. Director will dictate external communication.

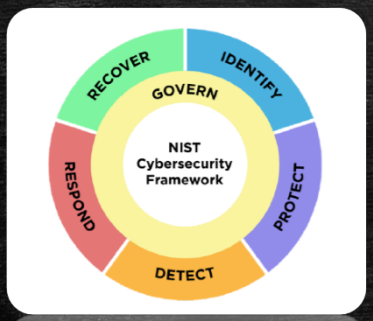
44

Bringing it all together

- We know the risks
- We have a team
- We have done the initial assessment of risks vs our environment
- We have core concepts decided
- So now what?

45

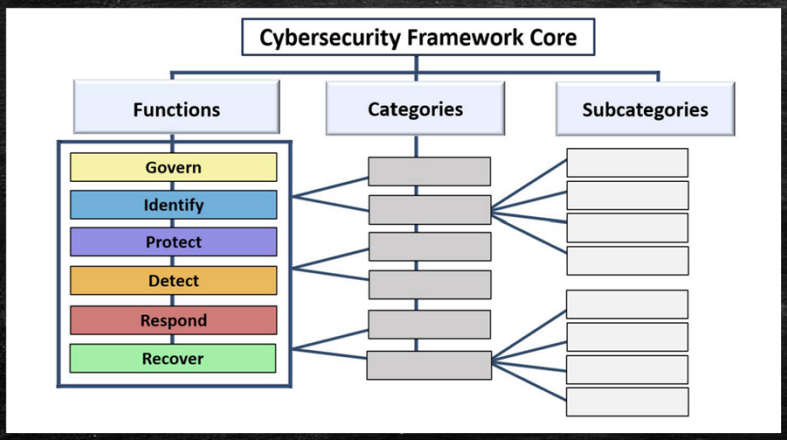
NIST 2.0 Framework



https://www.nist.gov/cyberframework

46

NIST 2.0 Framework



47

NIST 2.0 Framework

At a top level, frameworks outline key components of a documented *plan*.

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

48

NIST 2.0 Framework

ID.AM

Each section can have applicable subsections. All are not required – just what makes sense.

Each subsection could be a paragraph or much more, depending on the subject.

IDENTIFY (ID): The organization's current cybersecurity risks are understood

- **Asset Management (ID.AM):** Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy
  - **ID.AM-01:** Inventories of hardware managed by the organization are maintained
  - **ID.AM-02:** Inventories of software, services, and systems managed by the organization are maintained
  - **ID.AM-03:** Representations of the organization's authorized network communication and internal and external network data flows are maintained
  - **ID.AM-04:** Inventories of services provided by suppliers are maintained
  - **ID.AM-05:** Assets are prioritized based on classification, criticality, resources, and impact on the mission
  - **ID.AM-07:** Inventories of data and corresponding metadata for designated data types are maintained
  - **ID.AM-08:** Systems, hardware, software, services, and data are managed throughout their life cycles

49

CSF for your department

- Make it your own – it does not need to be 100 pages!
- Tie the CSF for radiation oncology into the larger picture of your institution
- The plan should be updated at least annually
- The IRT should drill – with "live" exercises and with tabletop exercises.

50

Challenges and the Future

- Hospital IT does not always know what Radiation Oncology is
- Hospital Admin may not be invested
- Lack of realistic risk appetite
- Lack of time to document and drill
- Many vendors and medical devices – lack of functionality

51

Challenges and the Future

- AI will speed both attacks and response
- AI will improve coding and minimize inherent risks
- Systems will get better at self protection and healing
- Legal actions will continue to motivate proper behavior
- Vendors will become more of a partner and IHE-RO / RTSEC will fix legacy issues

52

General Advice for Cybersecurity

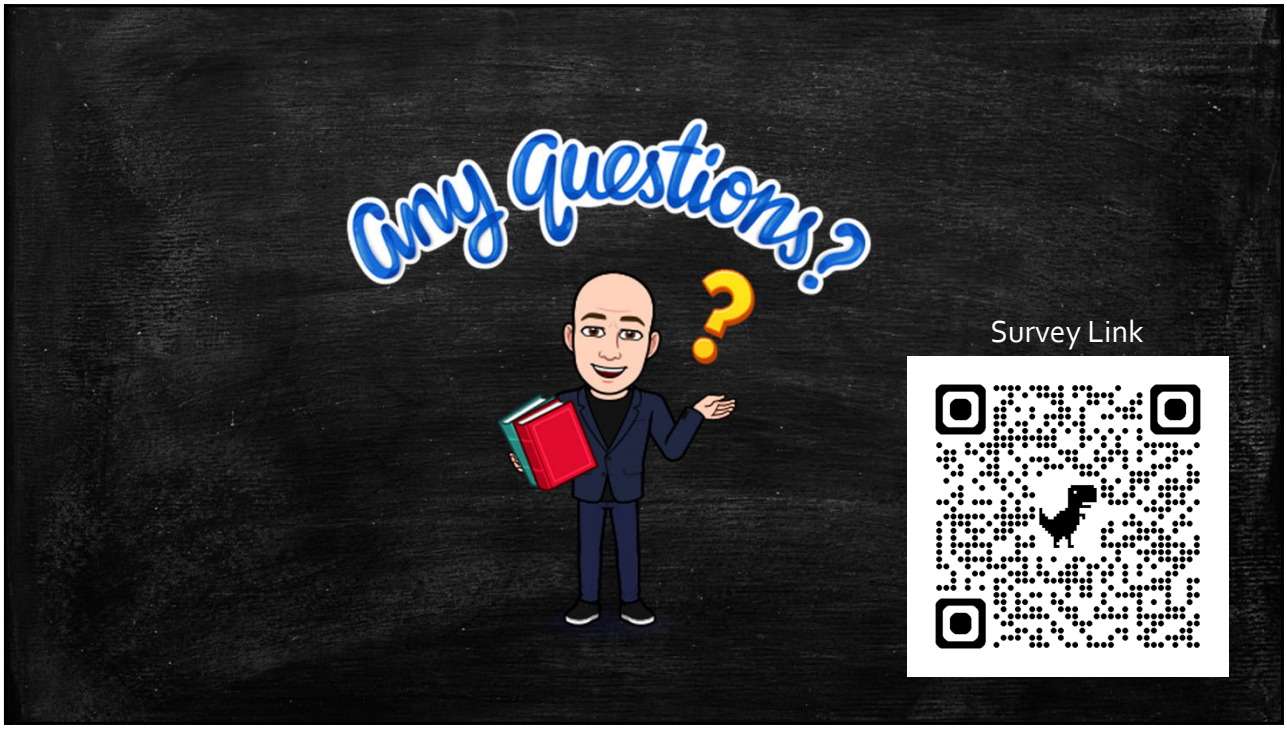
- Minimize handling email on phones – hover over links on computer.
- Don't ever be rushed, and always verify.
- Don't trust just any QR code (except mine).
- Update your phones and computers.
- Reboot your home routers every week.
- Backup important data (and TPS plans!).

53

General Advice for Cybersecurity

- Don't respond to texts from unknown sources.
- Setup pass codes with family and others if it makes sense.
- Use passkeys when offered the chance and a password program like Keeper.
- Keep NFC off if not in use. BT is probably unavoidable.
- Lock your SIM cards, as well as your credit bureaus.

54



55