

Cybersecurity and AI in Senior Living:

What You Need to Know

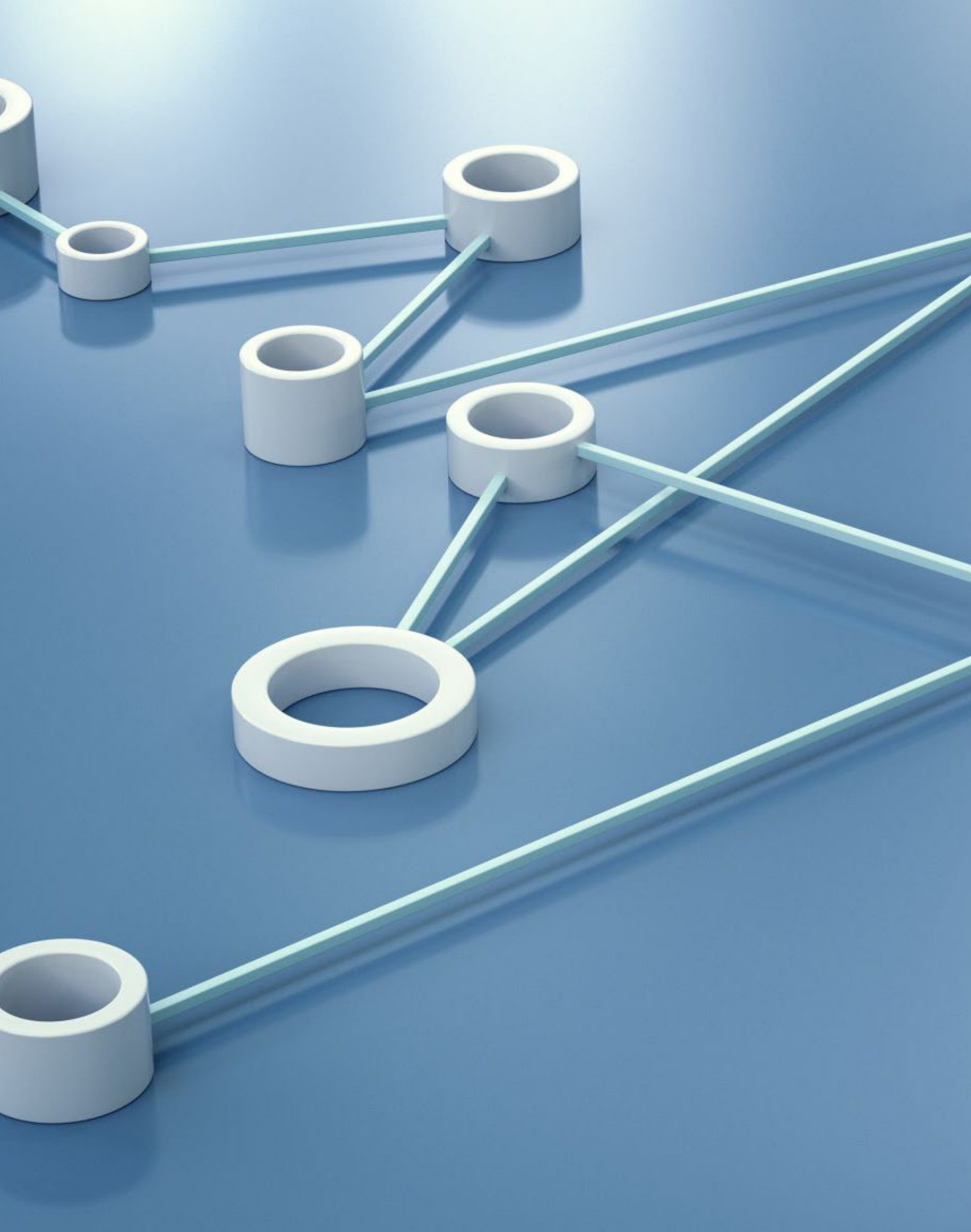
John DiMaggio, CEO
Blue Orange Compliance





Agenda

- Cybersecurity and HealthCare
- Artificial Intelligence in Senior Living
- Cybersecurity and AI
- What to do Now



Why Is Healthcare A Target?

- Relatively weak defenses
- Valuable Data
- Operational Urgency
- Numerous interfaces and sharing
- Everyone is a target and no one is a target

Cybersecurity

You have
Something
Valuable

- Sensitive information
- Protected information
- Ability to operate business using technology
- Reputation
- Money, cyber insurance

Cyber criminals

- In business to make money
- Have tools, knowledge, tradecraft, AI

Other Factors

- Human Error
- Accidental, Environmental, Vendors
- Storms, Tornados, Floods

- Confidentiality
- Integrity
- Availability

Common Attack Vectors (Ways Bad Guys Get In)

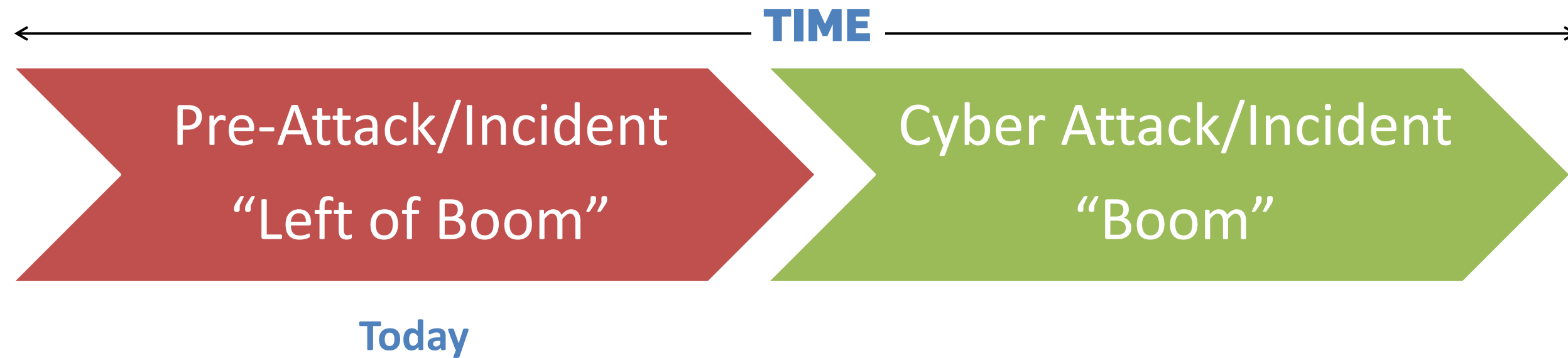
- You give them your password
- They guess your password
- Your password is on dark web
- Exploit known vulnerability (published but patch not applied)
- Click on bad link which installs malware on browser



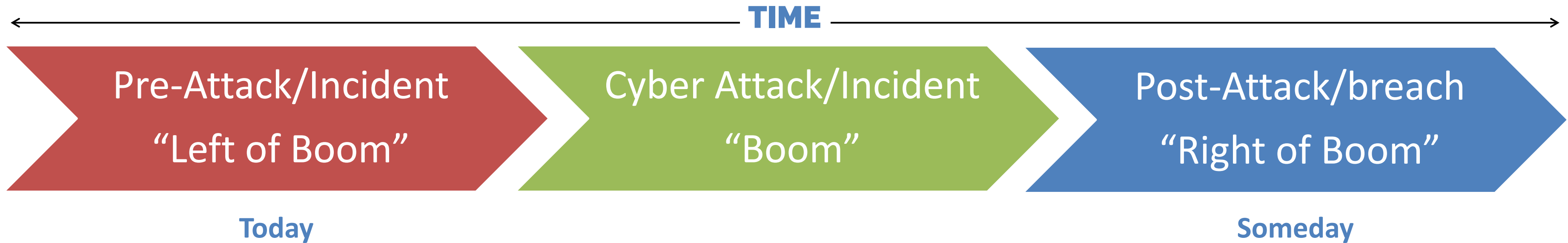
Cyber Attack/Incident Timeline – Left and Right of Boom



Cyber Attack/Incident Timeline – Left and Right of Boom



Cyber Attack/Incident Timeline – Left and Right of Boom



Cyber Attack/Incident Timeline – Left and Right of Boom



↑
TIME

Pre-Attack/Incident
“Left of Boom”

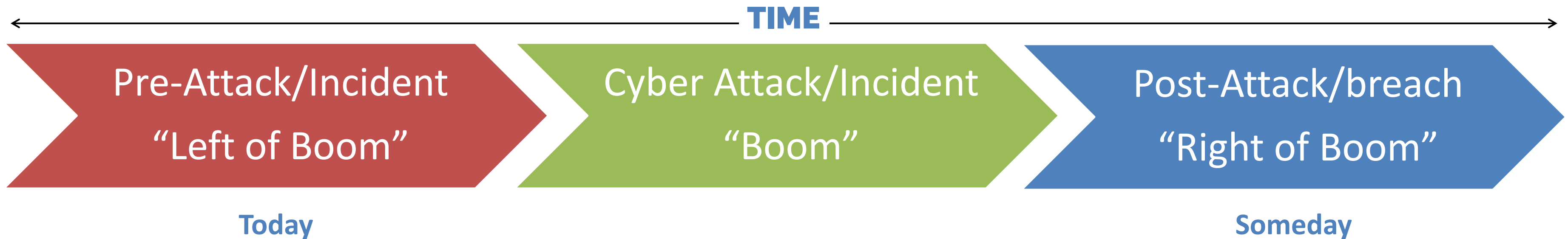
Cyber Attack/Incident
“Boom”

Post-Attack/breach
“Right of Boom”

Today

Someday

Cyber Attack/Incident Timeline – Phishing Example

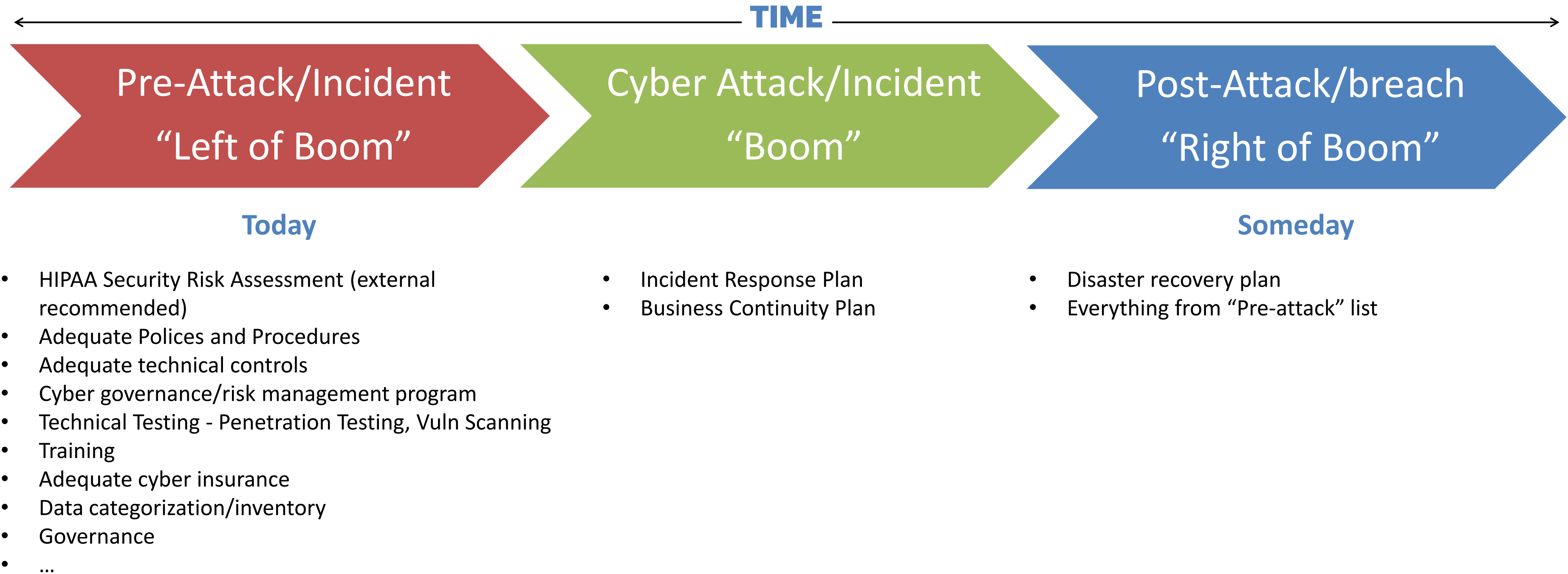


- Phishing email – User provided credentials
- Attacker gains foothold and cracks admin passwords
- Performs recon for files, systems high value data
- Installs ransomware software
- Downloads as much of your data as possible
- Once complete, triggers ransomware which encrypts data

- Users have trouble accessing systems
- Ransom note displayed with demand and contact info
- Contact cyber insurance
- Attempt to restore system
- Eradicate
- Contact threat actors regarding ransom amount
- Do they also have your data? Ask to provide proof.

- After party
 - Breach Notification for any affected residents
 - Civil lawsuits
 - HIPAA Office for Civil Rights (OCR) investigation

How to Prepare - Examples

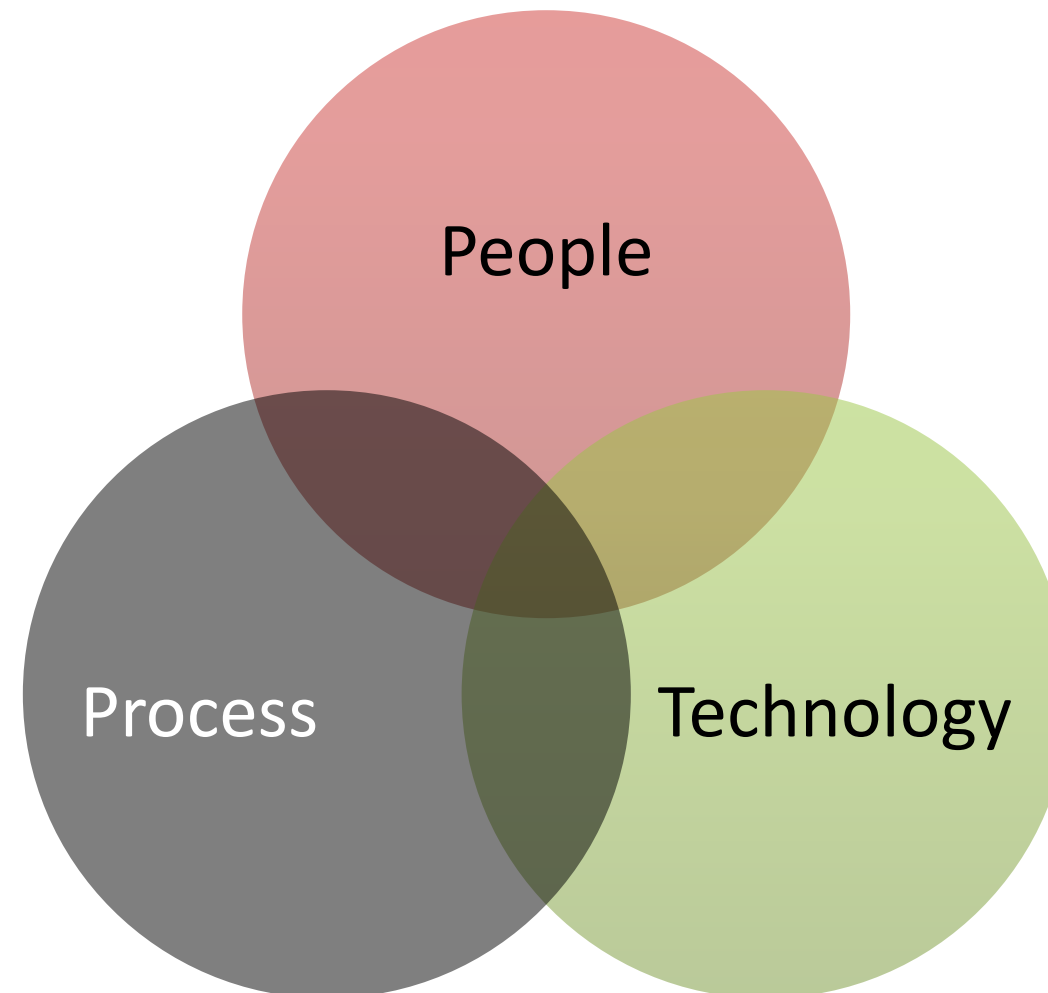
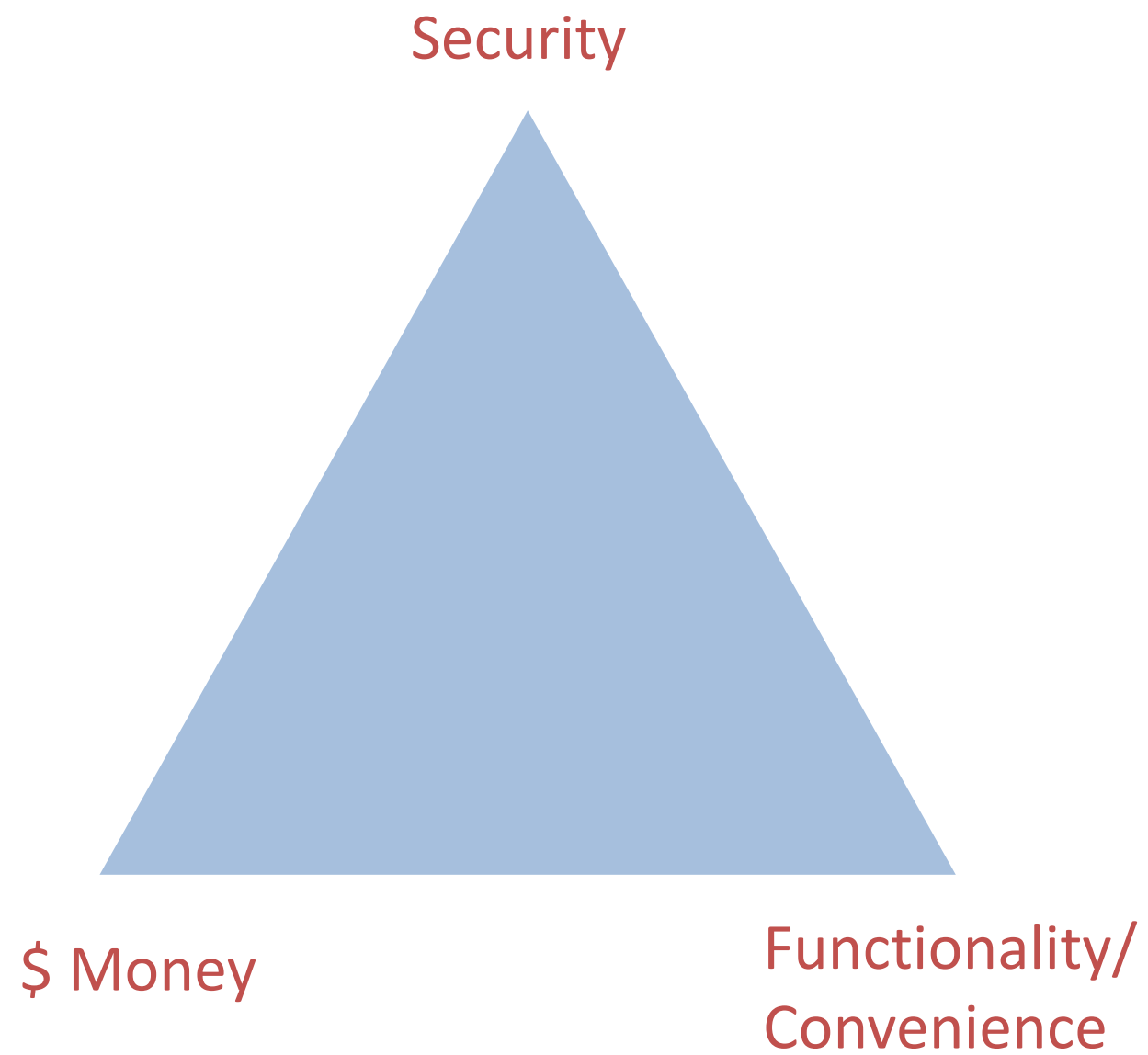


Stakeholders

- Residents/Patients and Their Families
- Employees
- Independent Contractors
- Management
- Board of Directors/Trustees
- Vendors, Business Associates
- Community
- Cyber Insurance Carrier
- Government
- Class Action Plaintiff Attorneys

Cyber Risk Management

Within Your Control



+



Evaluate Your Board's Role in Cyber Risk Management

Embed	Embed Cyber Risk in Strategic Decisions
Understand	Understand the Cyber Risk Management Program
Monitor	Monitor Cyber Resilience
Evaluate	Evaluate the Board's Cyber Oversight Allocation

HIPAA Security Risk Assessment- NOT Just an Assessment

Must be Documented

Scope and Data Collection

- Identification of systems (not just electronic health records and practice management)
- Data Mapping
- Use recognized framework (NIST – example)

Identification and Document Potential Threats and Vulnerabilities

- Threats: potential for a person or thing to trigger a vulnerability
- Vulnerabilities: flaw or weakness in system security procedures, design, implementation or internal controls
- Consider: Penetration and Vulnerability Testing
- Examples of Threats/Vulnerabilities: Ransomware, BEC, Flood, Lost Personal Device

Assess Current Measures and Likelihood of Threat Occurrence

- Documented Policies
- Documented Procedures
- Incident Response Plan
- Disaster Recovery/Business Continuity
- Document all threats and likelihood

Potential Impact of Threat Occurrence

- Criticality Assessment
- Magnitude of Impact

Determine Level of Risk

- Risk Levels
- Corrective Action Plans

Security Practices Terminology

- Reasonable Security Practices (Minimum)
 - “The HIPAA Security Rule sets standards for protecting electronic protected health information (ePHI) that are designed to ensure that covered entities (e.g., healthcare providers, health plans, and healthcare clearinghouses) implement appropriate safeguards to protect the confidentiality, integrity, and availability of ePHI.”
- Recognized Security Practices (Recommended)
 - Mitigation of Penalties
 - Improved Defense
 - Regulatory Compliance
 - Best Practices Under Section 405(d) of the Cybersecurity Act of 2015
 - Demonstrate that it has implemented recognized security practices for at least the previous 12 months

Security Practices Examples

Reasonable Security Practices (Minimum)

- Risk Analysis and Management
- Access Control Measures
- Encryption of ePHI
- Workforce Training and Security Awareness
- Incident Response Planning
- Physical Controls
- Technical Safeguards
- Third party/Vendor Management
- Backup and Disaster Recovery
- Patch Management

Recognized Security Practices (Recommended)

- Email Protection
- Endpoint Protection (ex SentinelOne)
- Access Management (ex MFA)
- Data Loss prevention
- Asset Management
- Network Management
- Vulnerability Management (ex penetration testing)
- Incident Response
- Medical Device Security
- Cybersecurity Policies (aligns with “Recognized”)

Cyber Insurance

Insurability Requirements/Key Factors

- Multifactor Authentication (MFA) - R
- Secure remote connectivity - R
- Segregated backups - R
- Employee training - R
- Cyber Incident Response Policies and Procedures - F
- Endpoint Detection and Response (EDR)/Intrusion Detection (IDS)/Next gen firewall - R for revenue exceeding \$50M, otherwise – F
- Encryption for data at rest and in transit - R/F

- Patch management - R
- Penetration Test/Vulnerability Scans - F
- Key vs non-key IT vendors - F
- Security Risk Assessments - F

R - Required

F - Favorable (more favorable underwriting, lower rates)

Cyber Insurance Policy Components

- Notification, credit monitoring, call center
- Network and information security liability
- Social engineering
- Fraudulent wiring instructions
- Consequential reputational loss
- Phishing
- Property business interruption and resulting physical damage
- Civil defense
- ...

Let's Talk About Data



- What are the Crown Jewels?
- Data
 - What is it?
 - Where is it?
 - In what form?
- Who Has Responsibility?
 - Not an IT thing – if the Operations Department has a Vendor Host, IT not Responsible

Data Categorizations and Locations

		Location/Storage			
		EHR	Devices	Shared drives/Cloud	Paper
Categories	Health Information	X	X	X	X
	Personal	X	X	X	X
	M&A/Legal		X	X	X
	Trade Secrets			X	
	Public	X	X	X	X

What You Need

Sufficient HIPAA Security Risk
Assessment

Ongoing Assessments, remediation
list, progress

Technical Testing

Cyber Risk Management Plan and
Process

HIPAA Security Rule Proposed Changes

- **Annual Risk Assessments** - Required, documented, NIST-aligned analyses

- **Stronger Technical Safeguards**

- Mandatory MFA
- ePHI encryption (in transit & at rest)
- Role-based access & least privilege
- Penetration testing, Vulnerability scanning
- Patching
- ...

Incident Management Enhancements

- **Business Associate Notification** - 24-hour notice after contingency plan activation
- **Incident Response Plans** - Required policies for breach response, backups, and recover

Compliance & Oversight Updates

- **Annual Compliance Audits** – HIPAA SRA, Ongoing evaluations of security measures

- **Vendor Oversight**

Stricter control of third-party access to ePHI

-

What Is AI?

- Definition of Artificial Intelligence (AI)
 - AI refers to the simulation of human intelligence in machines
 - These machines are programmed to think and learn like humans
- Types of AI
 - Narrow AI: Designed for specific tasks
 - General AI: Possesses generalized human cognitive abilities
- Common AI Tools in Senior Living
 - AI-powered communication tools
 - Predictive analytics for resident care
 - Chat bots/agents



Types of AI being used in Senior Living

- Machine Learning – Monitors changes in daily routines
- Resident Voice control devices
- Fall detections
- Large language models (ChatGPT, CoPilot, etc.)
- Agentic AI

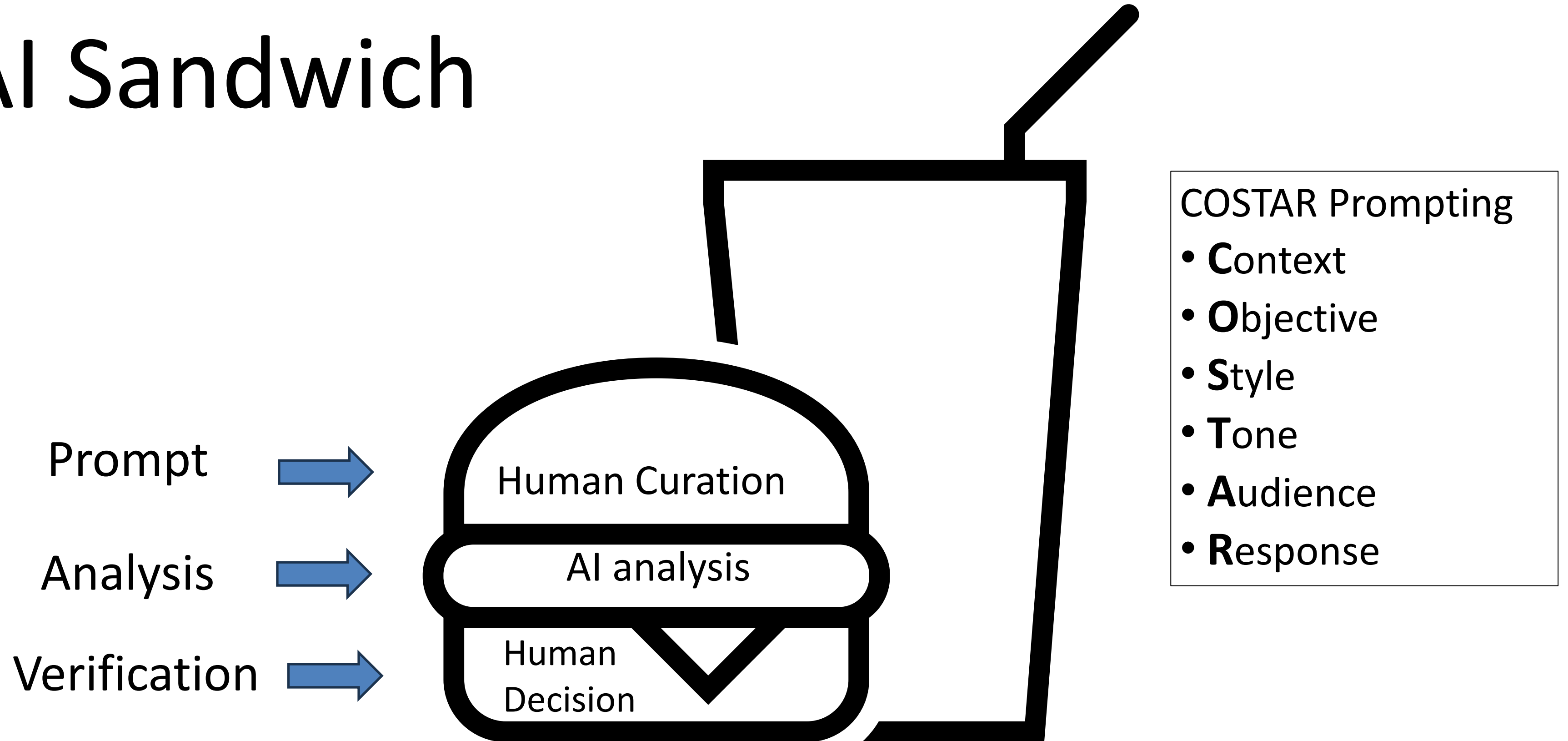


AI Potential Benefits - examples

- Workforce Optimization – Scheduling
- Financial Analysis & Summarization
- Fall reductions/Clinical
- Cost Control/Margin Protection
- General Research & Analysis
-



AI Sandwich



AI Potential Benefits - examples

- Workforce Optimization – Scheduling
- Financial Analysis & Summarization
- Fall reductions
- Cost Control/Margin Protection
- General Research & Analysis
-



Arrows and Guns

Bad Guys

- Deep fakes (voice/video)
- Auto spear-phishing
- Create malware insertion
- Defeat good guy defenses
-

Good Guys

- Deep fake detection
- Malicious code detection
- Incident response
- Predictive Analysis
-

Operational Risks

- Over-reliance on AI
 - Dependence on AI for critical decisions
 - Potential for errors without human intervention
- Lack of Human Oversight
 - Inappropriate outcomes due to insufficient monitoring
 - Need for human judgment to ensure accuracy



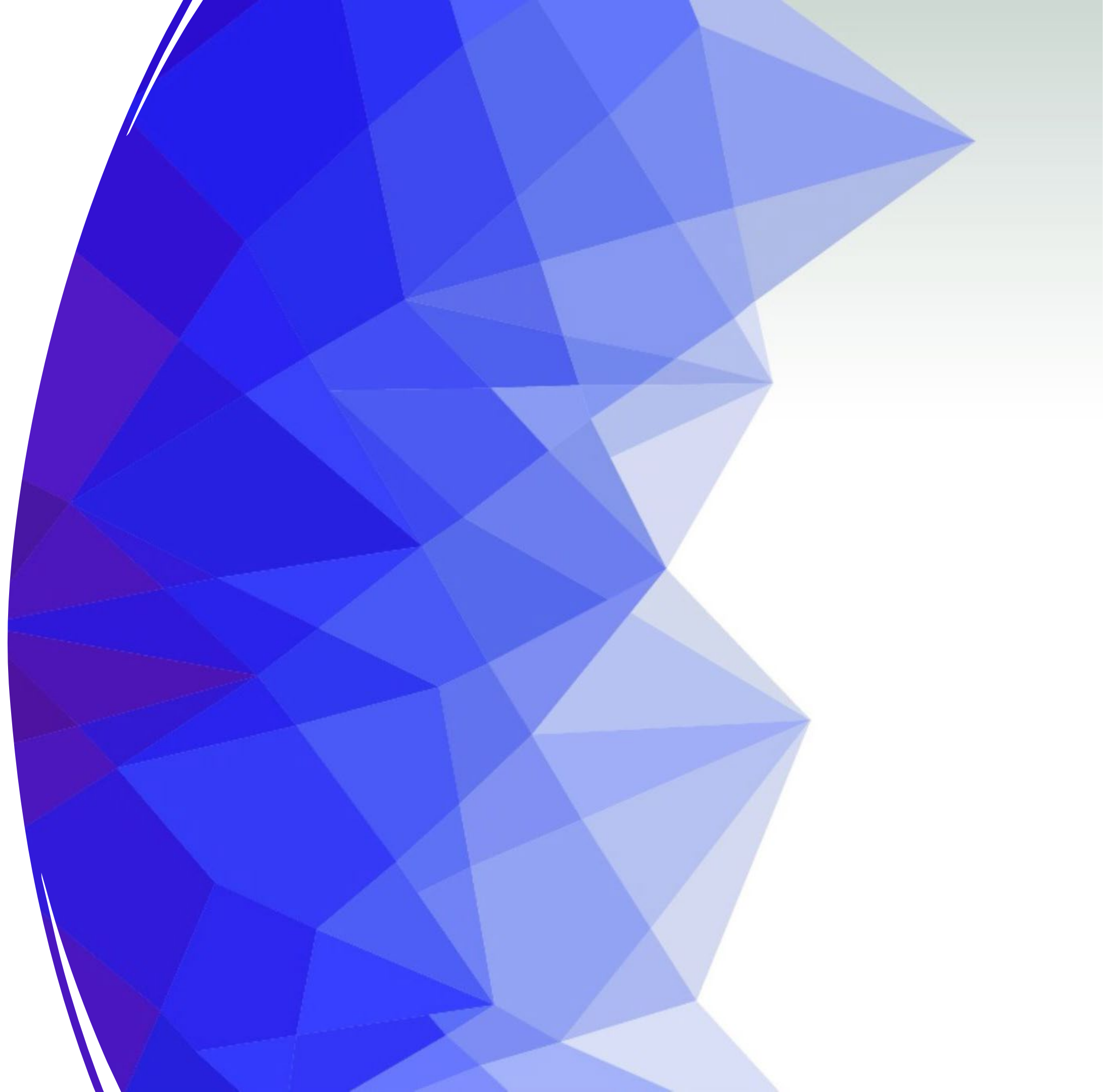
Legal and Compliance Risks

- Shadow AI
- Data privacy concerns
- HIPAA compliance
- AI-generated content
- Potential misinformation
- Ethical Considerations
 - Ensuring AI decisions respect resident dignity
 - Maintaining autonomy



Implement Usage Policies

- Develop Clear Policies for AI Use
 - Ensure policies are well-defined and accessible
 - Provide examples of acceptable AI applications
- Define Appropriate and Inappropriate Uses of AI Tools
 - Outline specific scenarios where AI can be beneficial
 - Highlight potential misuse and its consequences



GENERATIVE ARTIFICIAL INTELLIGENCE USE POLICY**Updated 19 February 2025****1.0 Purpose**

The purpose of this policy is to establish guidelines and best practices for the responsible and secure use of generative artificial intelligence (AI) within our organization ("we" or "us"). Generative AI refers to technology that can generate human-like text, images, or other media content using AI algorithms, such as ChatGPT, Google Gemini and Microsoft CoPilot (collectively, "AI").

2.0 Scope

This policy applies to all employees, contractors, and third-party individuals who are providing services for our organization.

3.0 Risks

- AI tools available on the web are not private. Any data you submit to an AI tool may be used for training the AI model and could become available to other users.
- AI's training data may include copyrighted materials and violate the rights of others.
- AI tools may provide biased results based on their training and data.
- AI tools are not accurate. Information may be outdated, misleading, or fabricated.

4.0 Prohibited Use

You may not use AI in the performance of your services, or submit any information about our organization, such as information about our business, our users, employees, customers, or vendor without express written permission by our IT team and management.

5.0 Approval Required for AI Use

- Our IT team and senior management must evaluate and approve any use of AI.
- Our evaluation process must include a review of the tool's security features, terms of service, privacy policy and assuring that such tools meet the AI Risks and Trustworthiness Framework offered by the National Institute of Standards and Technology.

6.0 Compliance with Laws and Regulations

All users of AI must comply with applicable laws, regulations, and ethical guidelines governing intellectual property, privacy, data protection, and other relevant areas. We prohibit unauthorized use of copyrighted material or creation of content that infringes on the intellectual property of others.

7.0 Responsible and Ethical Use

Your use of AI must align with our values, ethics, and quality standards. Do not use AI content that is misleading, harmful, offensive, or discriminatory.

8.0 Acceptable Use

You may use approved AI platforms solely for specific tasks and data authorized by us. Unless we provide otherwise, do not input into any query or AI sensitive or protected data, such as:

• Sample Policy

Immediate Steps to Mitigate Risks



Implement Usage Policies

Develop clear policies for AI use
Define appropriate and inappropriate uses of AI tools



Train Staff

Provide training on AI tools and their limitations
Emphasize the importance of human oversight and ethical considerations



Establish Monitoring Protocols

Regularly review AI outputs
Assign responsible staff members to oversee AI-generated content

Train Staff

Training on AI Tools

- Provide comprehensive training on the use of AI tools
- Explain the limitations of these tools

Human Oversight

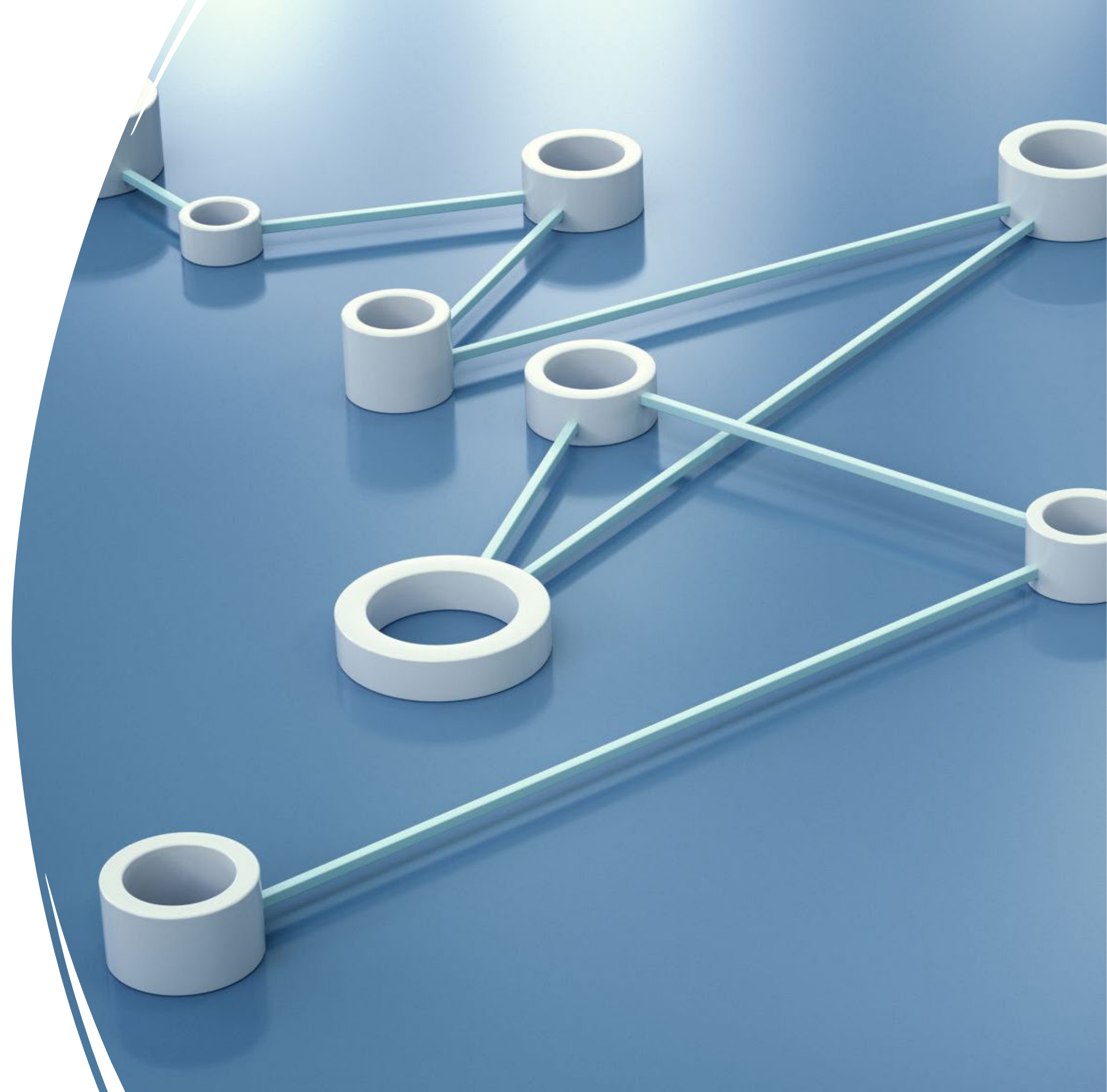
- Emphasize the necessity of human oversight in AI operations
- Discuss scenarios where human intervention is crucial

Ethical Considerations

- Highlight the ethical aspects of using AI
- Ensure staff understand the ethical implications of AI decisions

Establish Monitoring Protocols

- Regular Review of AI Outputs
 - Ensure accuracy and relevance of AI-generated content
 - Identify and address any anomalies or errors
- Assign Responsible Staff Members
 - Designate team members to oversee AI content
 - Ensure accountability and proper management



Enhancing Data Privacy and Security

- Review Data Handling Practices
 - Ensure AI tools comply with HIPAA and other regulations
 - Conduct regular audits of data handling practices
- Strengthen Cybersecurity Measures
 - Implement AI-specific cybersecurity protocols
 - Monitor for AI-related security threats and respond promptly



Building a Sustainable AI Strategy

- Regular Audits
 - Ensure AI tools and outputs are consistently evaluated
- Continuous Staff Education
 - Keep staff updated with the latest AI policies and practices
- Collaboration with Legal and IT Teams
 - Stay ahead of regulatory changes through teamwork



Thank You!

John DiMaggio, CEO

Blue Orange Compliance

John.dimaggio@blueorangecompliance.com

614.567.4109

