

# **CYBERSECURITY & RESILIENCE IN SMART MANUFACTURING**

Kristen M. Pope – General Manager,  
Gates Machine Tool Repair




# **Setting the Scene: Why Business Continuity Needs to Evolve**

# Traditional vs. Modern Business Continuity Challenges

Category	Traditional Challenges	Modern Challenges
Primary Risks	Natural disasters, power outages	Cyberattacks, IoT failures, ransomware
Continuity Focus	Physical infrastructure recovery	Cyber resilience, data protection
Tech Dependence	Minimal digital reliance	Heavy use of cloud, IoT, AI
Response Time	Slower, manual recovery	Real-time monitoring & automation
Plan Updates	Annual or infrequent reviews	Ongoing updates for cyber risks
Testing & Training	Physical drills, tabletop exercises	Cyber simulations, system testing
Security Concerns	Theft, fraud, physical risks	Data breaches, ransomware, insider threats





# Impact of Digital Transformation & Industry 4.0

## The Role of Automation, IoT, and AI in Manufacturing

Automation: Streamlines production, increases efficiency, and reduces human error.

IoT (Internet of Things): Connects machines and systems for real-time monitoring and predictive maintenance.

AI (Artificial Intelligence): Optimizes decision-making, enhances quality control, and enables smart manufacturing.

New Risks: Increased connectivity and reliance on digital systems introduce cybersecurity, system failure, and data integrity challenges.





# Recent Disruptions in Smart Manufacturing

Cyberattacks: Ransomware attacks on manufacturers leading to halted production.

System Failures: Software bugs and IoT malfunctions causing unexpected downtime.

Supply Chain Disruptions: Semiconductor shortages and logistics failures impacting production.

# **Identifying Gaps in Current Business Continuity Practices**

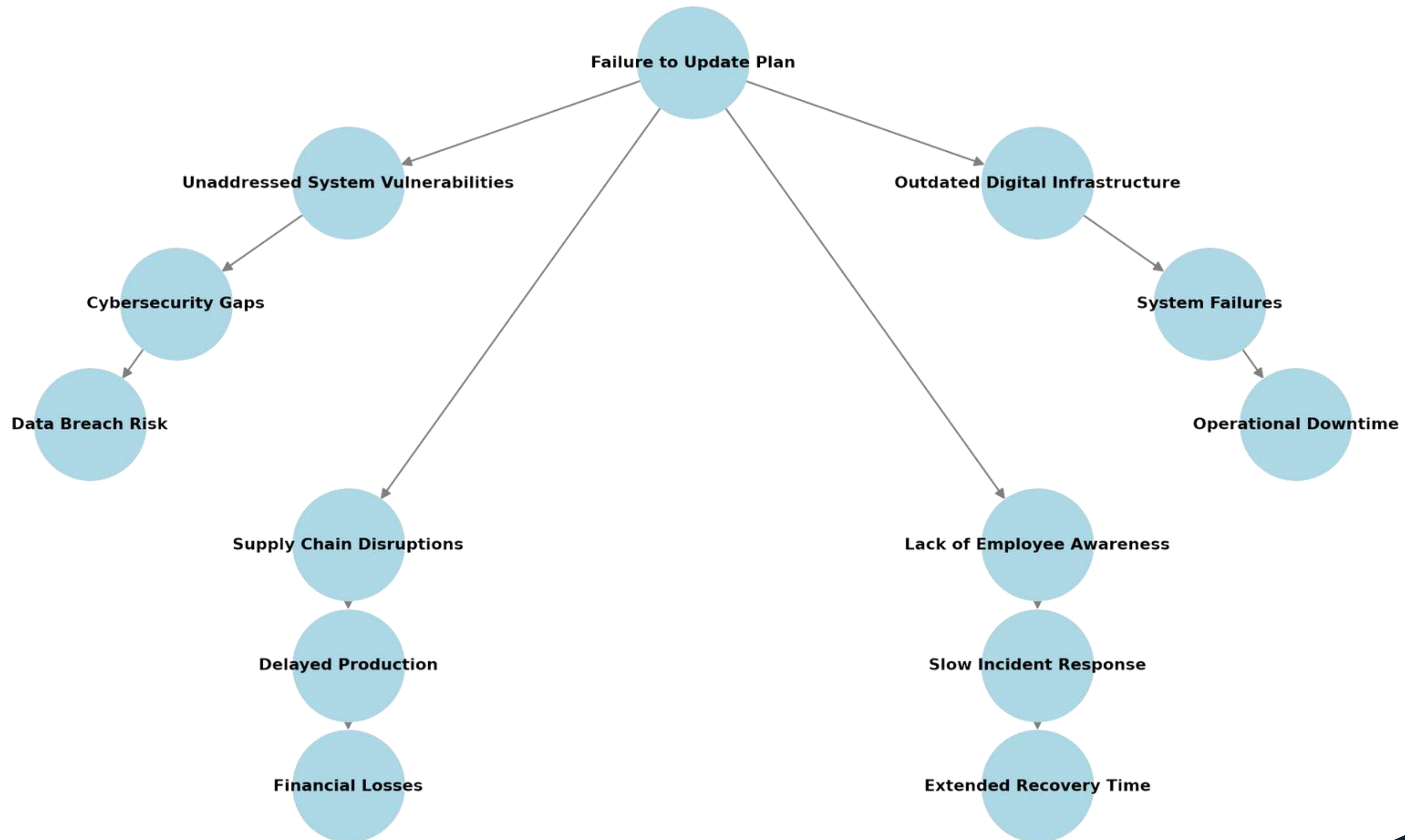


# Why Organizations Fail to Update Plans

- **Complacency** – false sense of security
- **Lack of Awareness** – uninformed leadership and staff
- **Budget Constraints** – insufficient financial resources
- **Time & Resource Limitations** – prioritizing daily operations
- **Failure to Conduct Regular Testing** – unidentified weaknesses persist
- **Underestimating Emerging Threats** – overlooking new risks
- **Lack of Ownership** – no clear responsibility
- **Complexity of Modern Business Operations** – evolving business challenges



# Risks of Outdated Continuity Plans





# Open Discussion

“

How often do you  
revisit and test your  
continuity plan?



# **Digital Systems: Challenges and Mitigation**



# Risks of Failure in Digital Systems

## **IOT FAILURES: THE HIDDEN WEAK LINK**

Faulty sensors send bad data, leading to production errors, downtime, and equipment damage.

## **AUTOMATION BREAKDOWNS: A SINGLE FAILURE STOPS EVERYTHING**

One robotic or system failure can halt entire production lines, causing costly delays.

## **SOFTWARE VULNERABILITIES: THE SILENT THREAT**

Unpatched software invites cyber threats, crashes, and data breaches that disrupt operations.

## **DATA DISRUPTIONS: WHEN INFORMATION BECOMES UNRELIABLE**

Network failures or cloud issues lead to incorrect inventory counts and unexpected stoppages.



## **SUPPLY CHAIN DELAYS: THE DOMINO EFFECT**

Small glitches like mislabeled shipments ripple through logistics, causing major slowdowns.

## **COMPOUNDING FAILURES: WHEN SMALL ISSUES BECOME EXPENSIVE PROBLEMS**

Minor technical failures left unchecked can escalate into major mechanical breakdowns and huge financial losses.

## **CYBERSECURITY RISKS: SMALL VULNERABILITIES, BIG ATTACKS**

Weak IoT security makes factories easy targets for hackers, leading to production sabotage.







# Digital Redundancy & Proactive Maintenance

Redundancy Across Critical Systems: Multiple layers of backups and failover systems to ensure no single point of failure.

Real-Time Monitoring & Predictive Analytics: Utilizing data-driven insights to anticipate issues before they lead to downtime.

Automated Recovery & Failover Processes: Seamless transition to backup systems in case of failure, minimizing operational disruption.

Distributed Infrastructure: Leveraging geographically dispersed data centers and cloud resources to maintain availability.

Continuous Testing & Drills: Regular simulation of failures to ensure the system's recovery processes are effective.

Scalable & Adaptable Design: Flexibility to expand and adjust as business needs evolve, maintaining continuity through growth or change.

Cybersecurity Integration: Protecting critical systems from cyber threats, ensuring data integrity and operational stability.

Employee Training & Awareness: Ensuring all staff are familiar with recovery processes and best practices for minimizing disruptions.



# Case Studies: Lessons from Digital Failures

## The Issue:

Boeing attempted to fully digitize the design and production of the 777X aircraft using advanced 3D modeling and digital twin technology. However, integration issues between legacy systems and new digital tools led to significant delays. The digital modeling failed to accurately predict manufacturing challenges, causing rework, supply chain disruptions, and FAA certification setbacks. The aircraft, initially set for 2020, is still not in service as of 2024.

## Lessons & Fix:

- Align Digital with Reality: Boeing adjusted its models to better reflect real-world manufacturing constraints.
- Strengthen Supplier Collaboration: Improved coordination ensured digital designs matched production needs.
- Prioritize Testing & Timelines: Future projects now include rigorous testing before full-scale implementation.



# **Cybersecurity as a Cornerstone of Continuity Planning**



# The Intersection of Cybersecurity & Business Continuity

## Cyber Risks in Continuity Planning:

Increasing reliance on digital systems and interconnected devices exposes organizations to significant vulnerabilities.

Cyberattacks (e.g., ransomware, data breaches) can disrupt operations and cause financial losses.

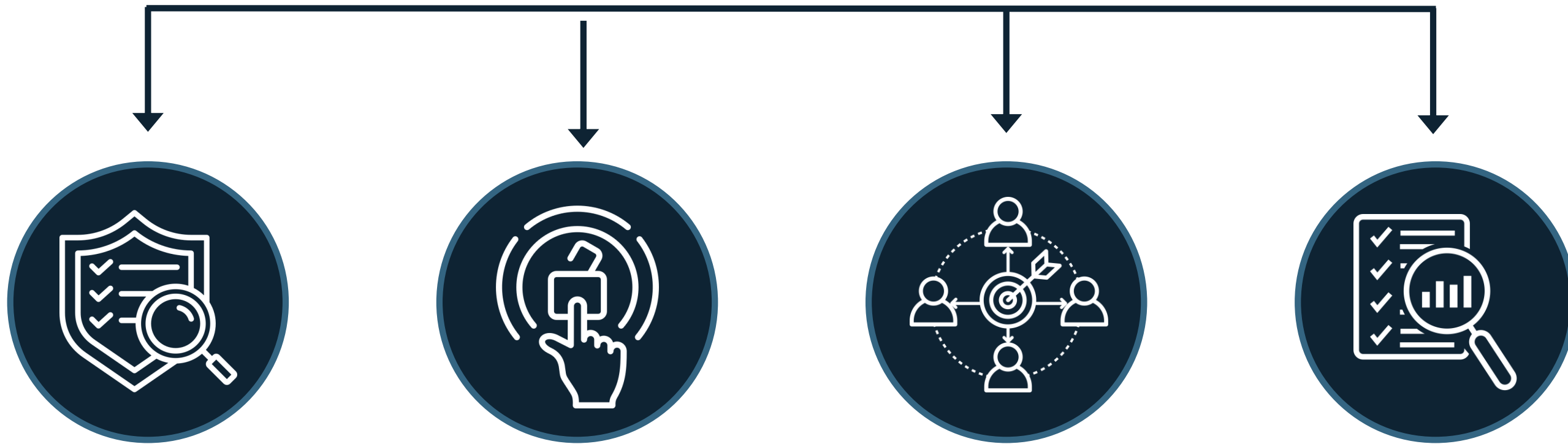
## Why Integrate Cyber Risks?

Cyber incidents can halt operations as effectively as physical disruptions (e.g., ransomware locking systems, data breach compromising processes)..

Integration ensures preparedness for both physical and cyber threats, minimizing downtime and protecting critical assets.



# Embedding Cybersecurity Risk Management



## Regular Audits

Conduct frequent audits to identify and address vulnerabilities, ensuring compliance and securing all entry points.

## Access Control

Implement strict policies around access rights, ensuring that only authorized personnel can access sensitive data and systems.

## Employee Training

Consistently educate employees on the latest cybersecurity threats, safe practices, and how to recognize suspicious activity.

## Continuous Risk Assessments

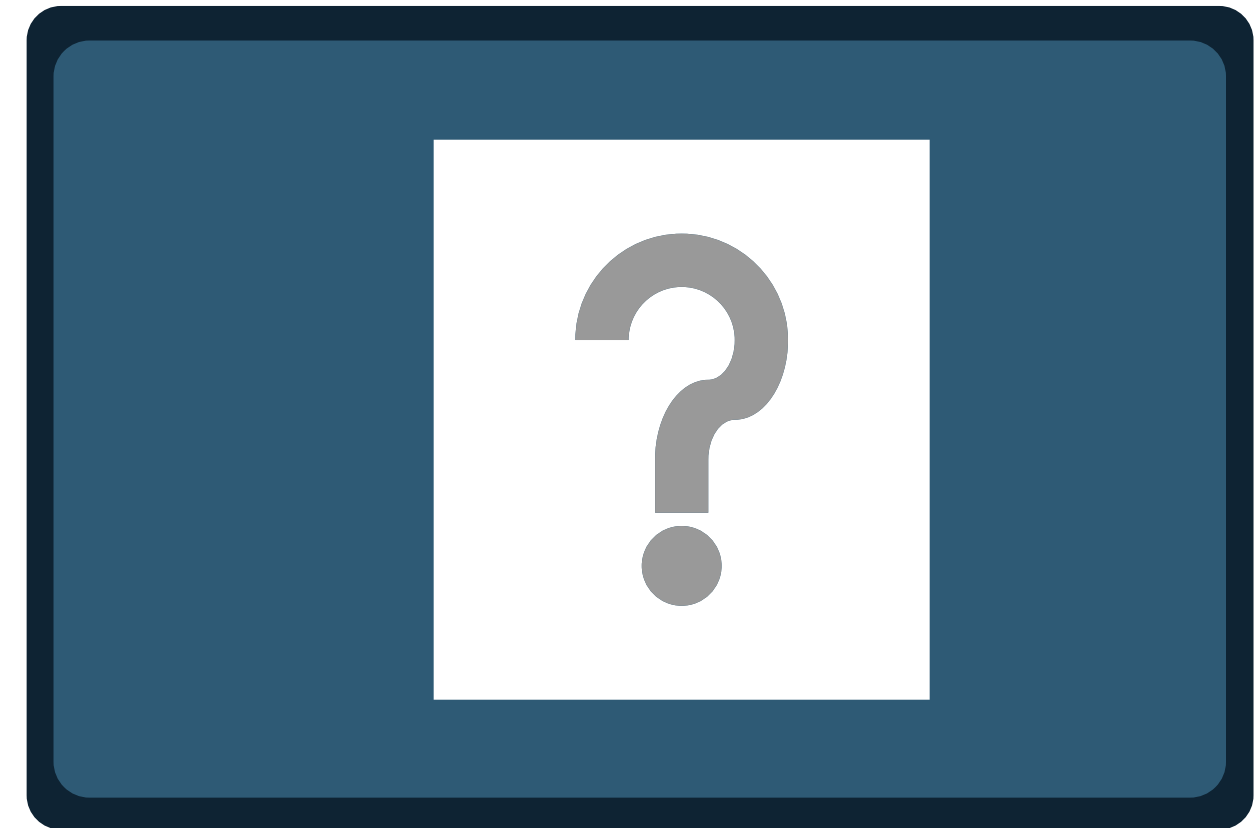
Cyber threats evolve, and risk assessments must be updated regularly to stay ahead of new challenges.



# Collaborative Exercise

“

How would your  
organization respond  
to a cyberattack?



# **Building Awareness & Engagement Across the Organization**





# Ensuring Employees Understand Business Continuity Plans

1. Regular Training – Conduct quarterly sessions with exercises and simulations.
2. Role-Specific Training – Focus on individual responsibilities during disruptions.
3. Cross-Training – Train employees across departments for flexibility.
4. Engaging Content – Use gamification and simulations to boost retention.
5. Consistent Messaging – Communicate regularly via emails, newsletters, and meetings.
6. Two-Way Communication – Encourage feedback and Q&A sessions.
7. Redundant Channels – Use text and apps for backup communication.
8. Leadership Engagement – Leaders should model BC behaviors and communicate its importance.

# Best Practices for Training Staff



## Set Clear Objectives

Define specific goals for each training session.



## Design Realistic Scenarios

Tailor exercises to reflect real-world challenges.



## Provide Hands-On Practice

Use simulations to build practical experience.



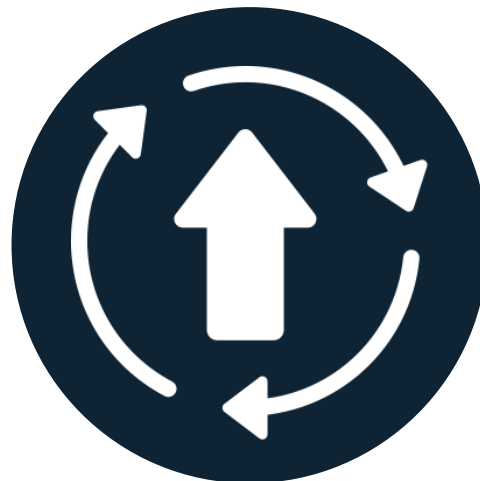
## Focus on Role-Specific Needs

Customize training for each department's responsibilities.



## Conduct Regular Reviews

Assess progress and gather feedback after each session.

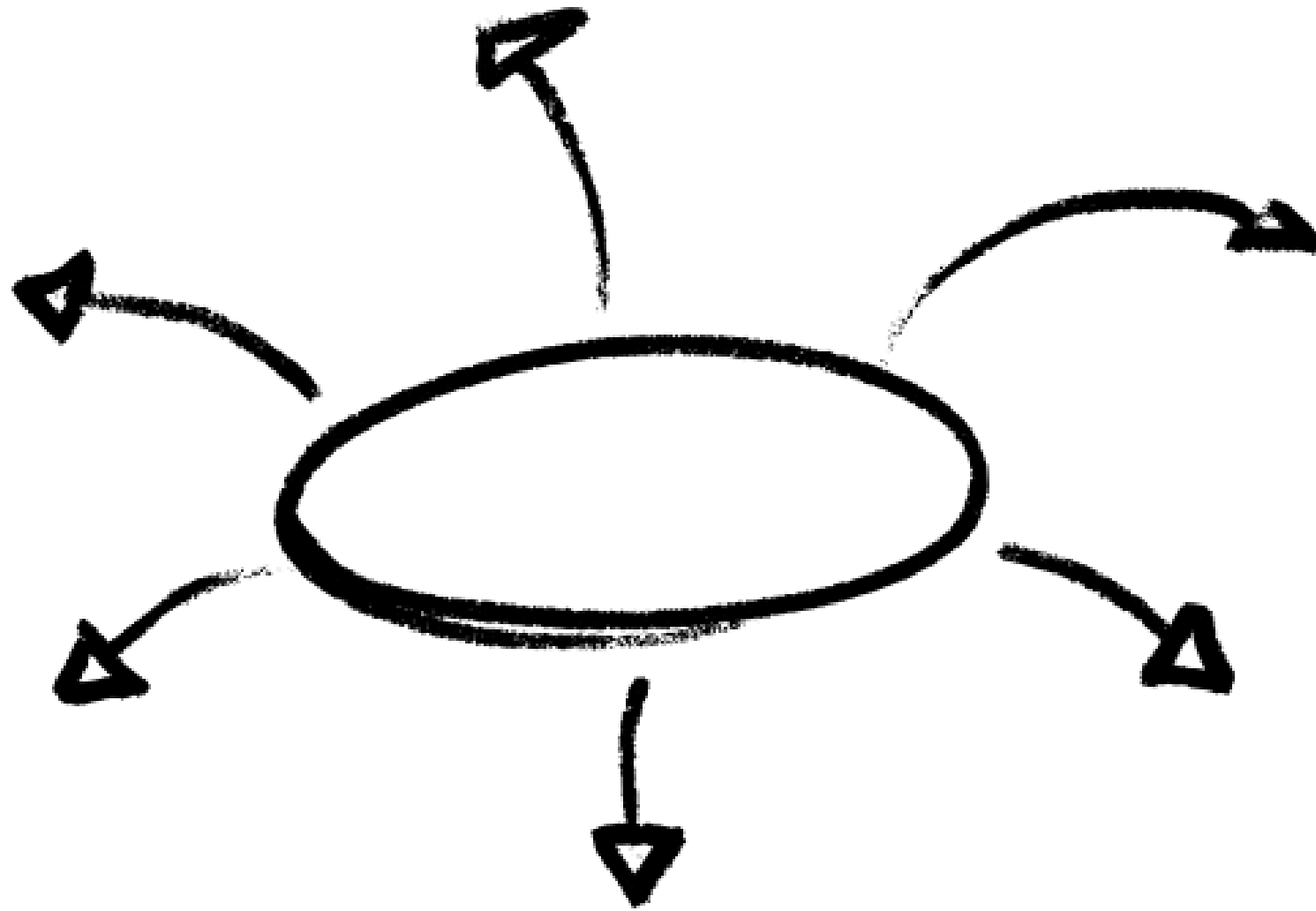


## Update Training Regularly

Refresh content to keep it relevant and effective.



# Workshop Exercise



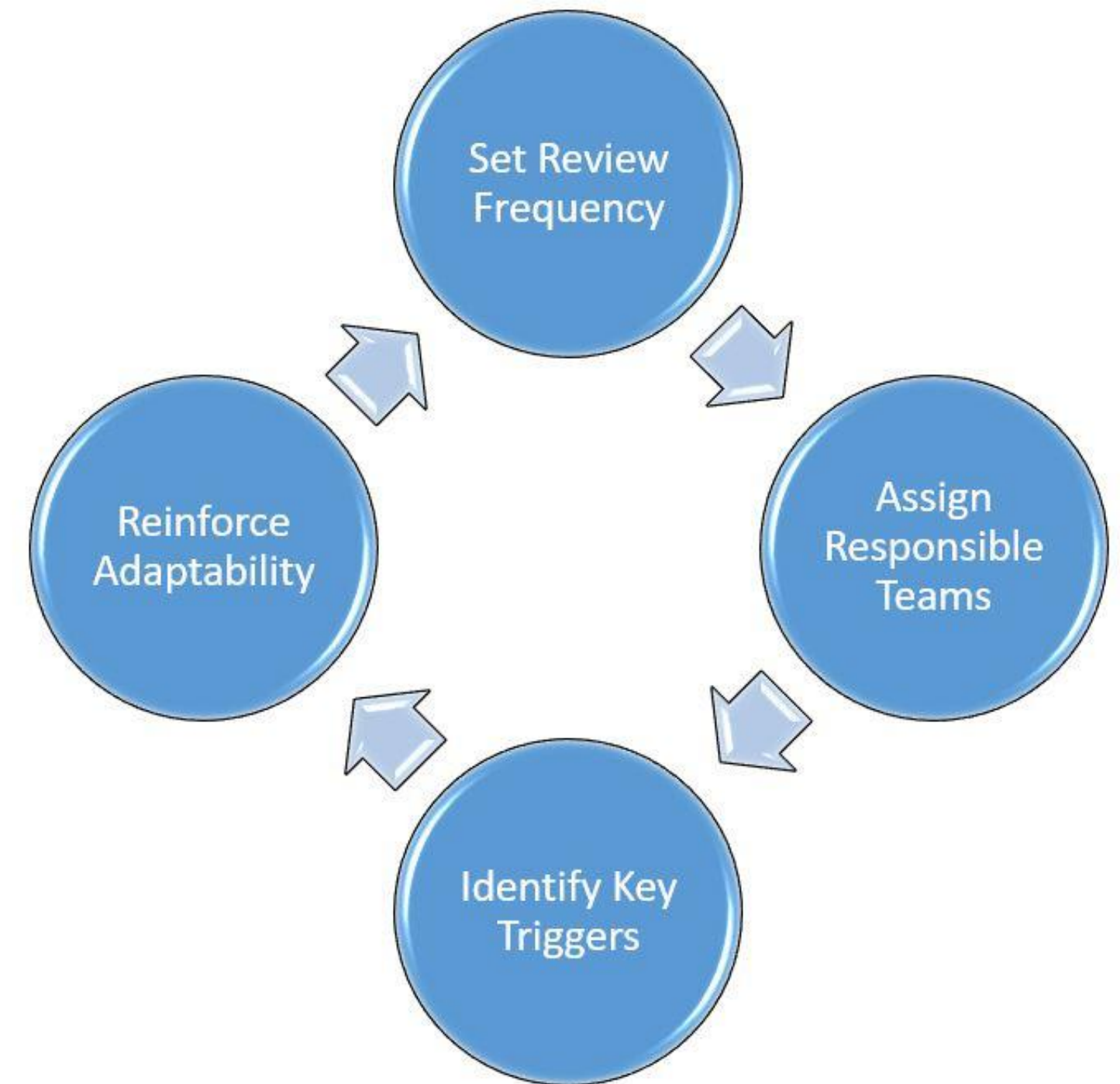
Brainstorm methods to increase  
internal awareness...



# **Actionable Takeaways: Building Resilience in the Digital Era**



# Steps to Regularly Review & Update Plans





# Tools & Frameworks for Preparedness

- Business Impact Analysis (BIA) – Identify critical processes & assess downtime impact
- Risk Assessments – Evaluate threats, assign risk levels, and refine response plans
- Software Solutions – AI-driven monitoring, BCM platforms, supply chain resilience tools
- User-Friendly Tools – Intuitive dashboards, real-time alerts, automated risk tracking
- Proactive Preparedness – Embed resilience into daily operations for rapid response





# Open Floor for Questions & Final Insights





**Connect with me**

