2025 KOnnect

Collaborative Cyber Resiliency Across IT, Cybersecurity, and Business Continuity

SPEAKER

Chris Chaisson (CBCP, CCRP)

Manager, Global Business Continuity Team | Applied Materials

CONNECTING RISKS THAT MATTER

APPLIED MATERIALS®

EDUCATION

The University of Montana
BS, Business Administration
Management Information Systems

Certified Cyber Resilience Professional

Certified Business Continuity Professional

HOBBIES & INTEREST

CAREER

KPMG — Business Continuity Consultant

resilinc — Director, Supply Chain Solutions

APPLIED MATERIALS — Material Innovation — Mgr. Global BCP Team

FOUNDED IN 1967

APPLIED MATERIALS™

World's Leading

semiconductor and display equipment company

$27.18 billion
Revenue

$3.2 billion
R&D spending

>22,000
Patents

~35,700
employees
in **24** countries

* Data as of fiscal year end, October 27, 2024

AGENDA

01 Introduction

02 Digital Concentration Risk

03 Cyber Resiliency vs Cybersecurity

04 The “Three-Legged Stool”

05 “Cyber-Forward” Business Continuity Planning

06 Q & A

Understanding “Digital Concentration Risk”

Digital Concentration Risk:

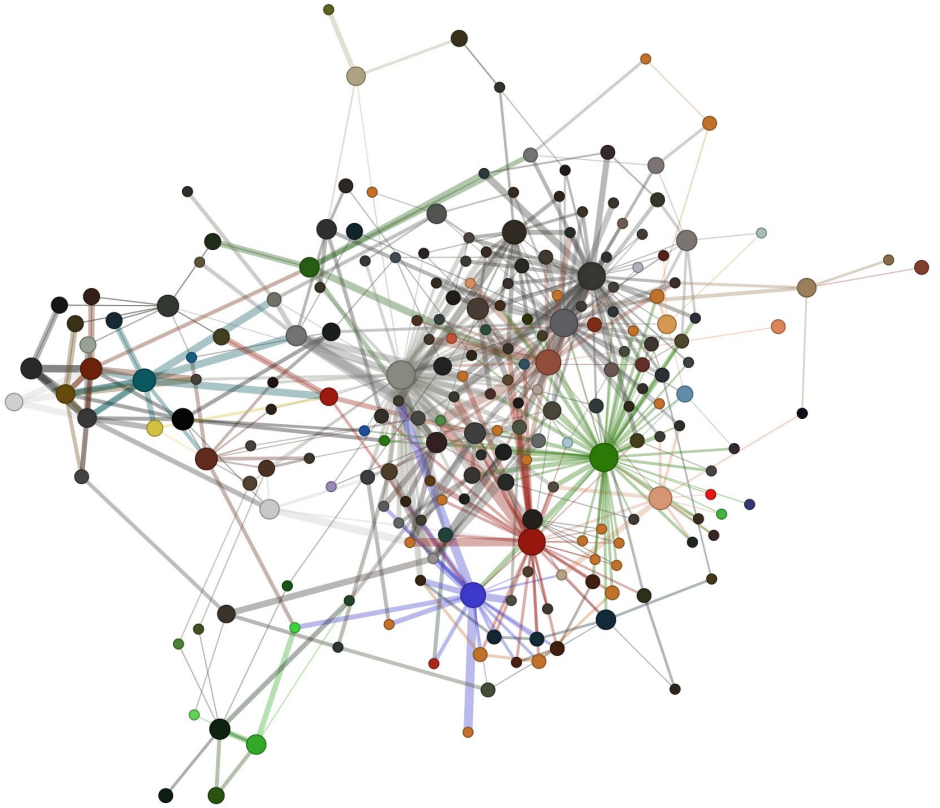
- Vulnerabilities arise

Why does it matter for cyber?

- A breach or failure in a concentrated area
- Interconnected systems
- Recovery is complex.
- Regulatory and Reputational Risk

Real World Example:

- 2024 CrowdStrike Outage



If one of your critical application is down for 2+ weeks, how would you continue operations?

Cyber Resilience

Cyber resilience is an entity's ability to **withstand**, **adapt** to, and **recover** from cyber threats and IT incidents & outages

- **Protect & Withstand**
- **Recover & Adapt**
- **Train the employes**
- **Exercise & Test**

Cybersecurity

Cybersecurity refers to the **preventive measures** and technologies used to protect systems, networks, and data from unauthorized access, attacks, or damage. It includes:

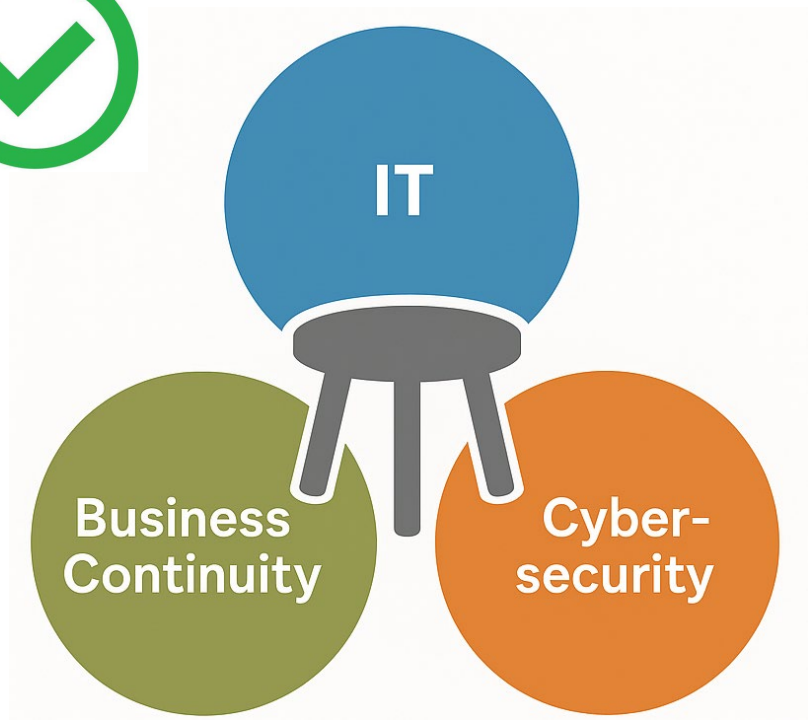
- Firewalls, encryption, and access controls
- Antivirus and anti-malware tools
- Identity and access management (IAM)
- Security policies and compliance frameworks
- The goal is to prevent breaches and protect data integrity and confidentiality

Key Differences: Cybersecurity vs. Cyber Resiliency

Aspect	Cybersecurity	Cyber Resiliency
Focus	Prevention	Continuity & Recovery
Goal	Stop attacks	Operate through and recover from attacks
Tools	Firewalls, IAM, encryption	BCP, DR, manual workarounds, recovery plans
Mindset	“Keep them out”	“Assume breach, stay operational”
Responsibility	Primarily IT & InfoSec	Cross-functional: IT, BCP, Cybersecurity, BUs

Cybersecurity Is About Protection, While Cyber Resiliency Is About Functionality During And After An Incident

The “Three-Legged Stool” Model

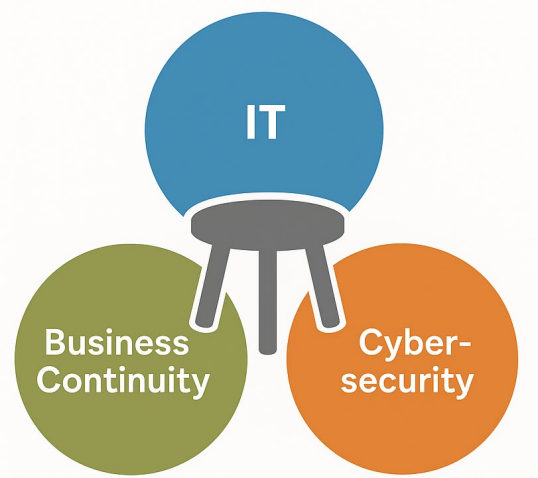


“A two-legged stool will stand, but only a three-legged stool offers true stability”

Importance of the “Three-Legged Stool” Approach

A three-legged stool method gives your company a holistic approach to cyber threats:

- Unified Response
- Gap Elimination
- Scalability and Resilience
- Stakeholder Confidence



Cyber disasters expose gaps in your strategy, do not wait to plan!

- Assess risks quarterly
- Involve business leaders, not just IT
- Create clear procedures and response actions for each team
- Schedule ongoing cross-functional BCP/IT/Cyber meetings
- Establish a dedicated cyber response team (cross-functional)
- Invite DR and IT stakeholders to BCP reviews and annual tabletop exercises

Cyber Resiliency Can Only Be Achieved If All Teams Work Together

2025 KOnnect

“Cyber-Forward” Business Continuity Planning

CONNECTING RISKS THAT MATTER

Preventive Strategies To Ensure Business Continuity

It's no longer a matter of "IF", but "**WHEN**" will an entity will suffer a cyberattack.

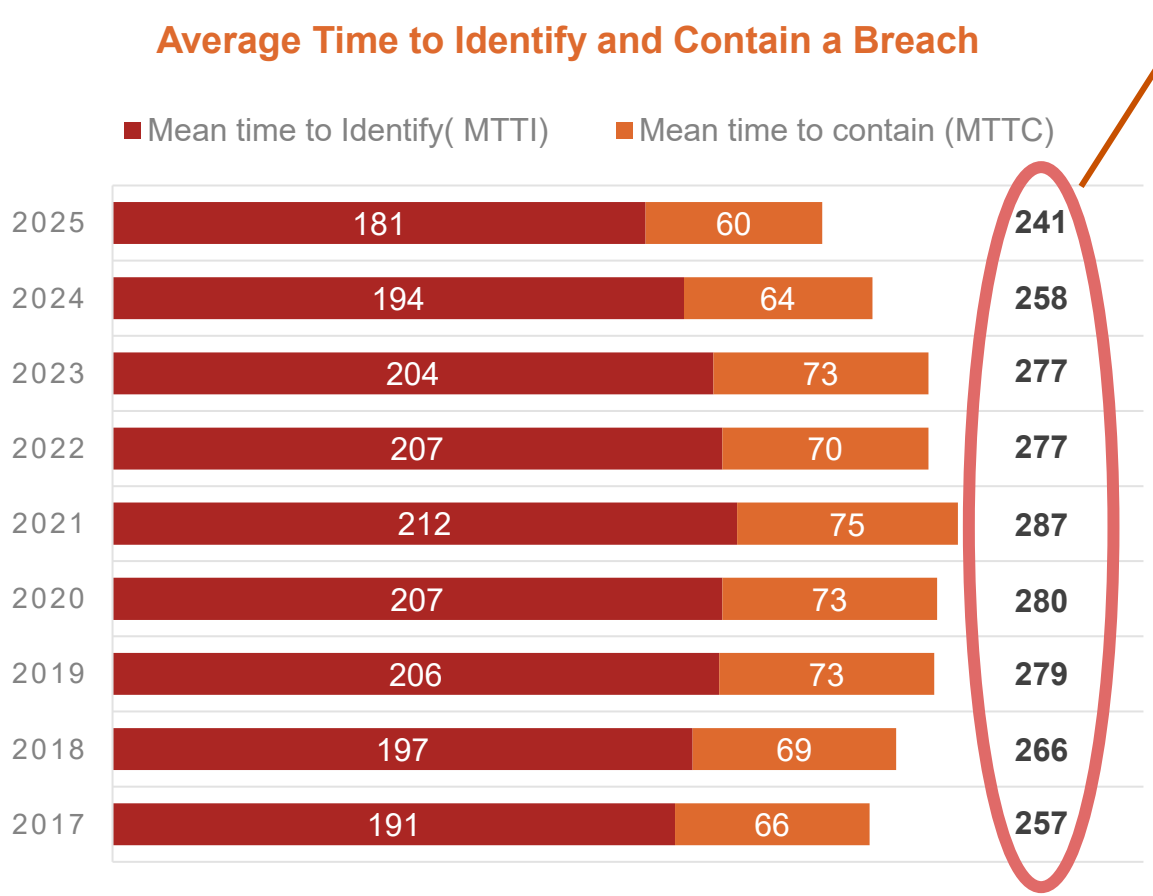
Assume that you have already been breached.

"There are two types of companies: those that have been hacked, and those who don't know they have been hacked."

Former CEO of Cisco - John Chambers

Cyber Incidents Differ From “Typical” Catastrophic Events

Minutes?... Hours?... **Days!!!**



Source: IBM Cost of Data Breach Report 2025

Pandemics

Natural Disasters

Accidents & Attacks

Network & System Outages

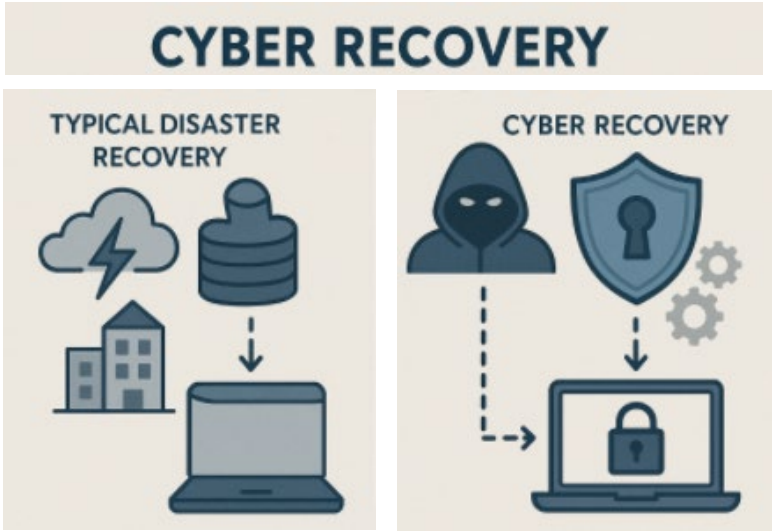
Communication & Power Outages

Transportation Issues

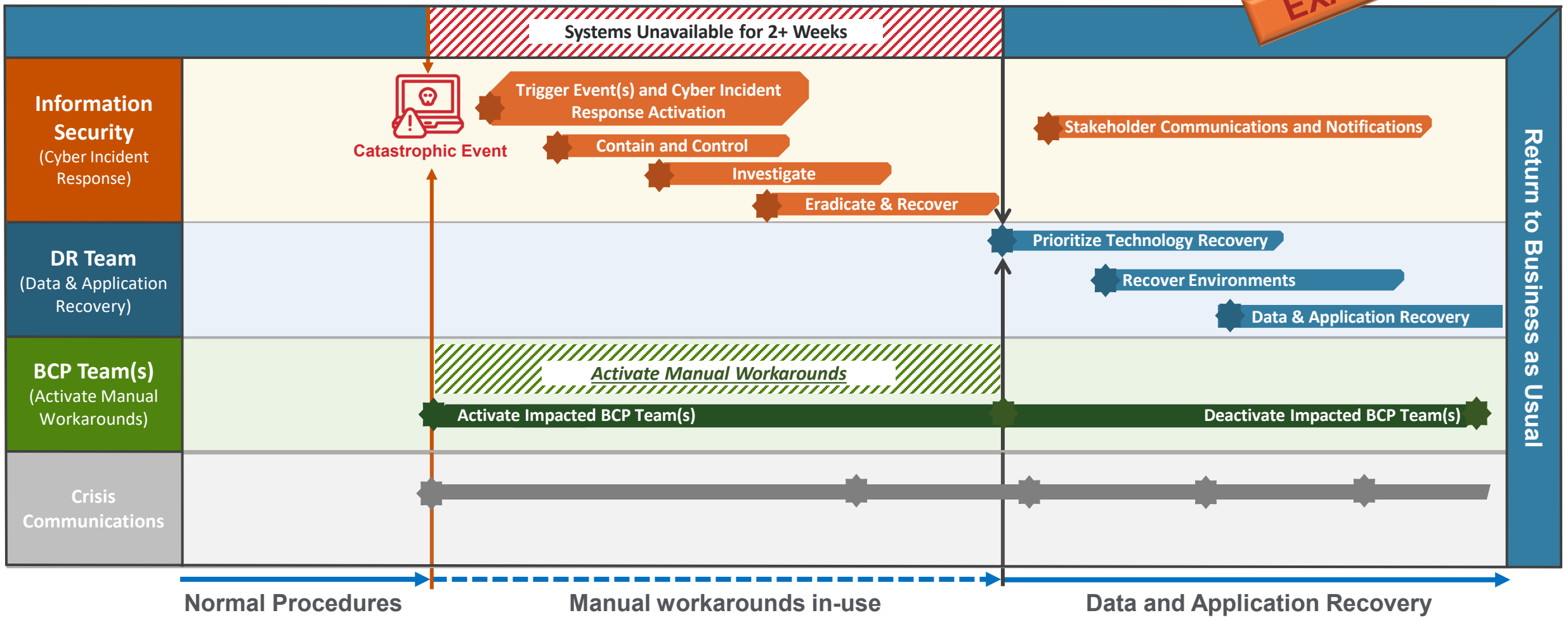
Traditional DR vs. Cyber Recovery

Key Recovery Strategy Differences

- **Backup Integrity**
  - Traditional DR assumes backups are safe and usable.
  - Cyber Recovery must validate backup integrity, often using immutable storage or air-gapped systems to prevent tampering
- **Recovery Point Objective (RPO) Uncertainty**
  - In a cyberattack, the exact point of compromise may be unclear.
- **Isolation and Security**
  - Cyber recovery emphasizes isolated recovery environments and forensic analysis to ensure malware isn't reintroduced during restoration
- **Cross-Functional Involvement**
  - Cyber incidents require collaboration across IT, cybersecurity, legal, communications, and business continuity teams.



The Challenge: Cyber Incident Response Timelines are Dynamic



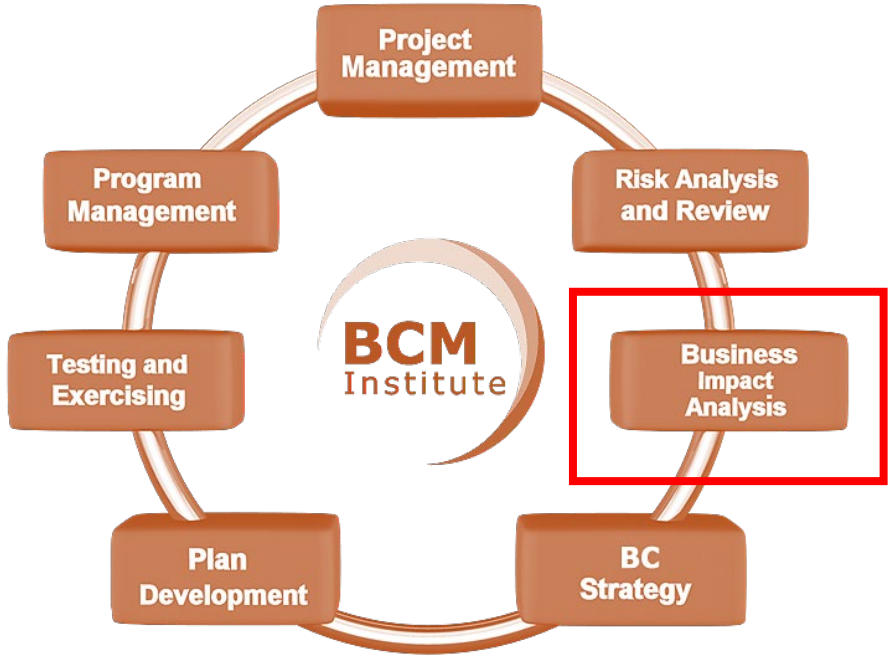
Sufficient manual workarounds are critical for business continuity during a catastrophic cyber event

Integrate Cyber Risks Into The Entire Business Continuity Planning Lifecycle

- Manual Workarounds and Extended Outage Planning
- Cyber Incident Response Integration
- Cross-Functional Collaboration
- Training and Exercises
- SaaS Risk Inclusion
- Governance and Executive Engagement

“Cyber-Focused” Business Impact Analysis (BIA)

- Historically, BIAs have been focused on:
  - People
  - Place
  - Technology
- Cyber-focused BIAs can help prioritize recovery efforts



Credit: BCM Institute

Cyber-focused BIAs shift the focus from physical and human dependencies to digital concentration risk, data integrity, and cyber threat scenarios.

Considerations for Cyber-Focused BIAs

1 Digital Concentration Risk

- Focus on vulnerabilities
- Highlight systemic risks

2 Tabletop Planning and Threat Modeling

- Incorporate specific cyber threats
- Evaluate business impact

3 Manual Workarounds

- Prioritize recovery sequencing
- Assess whether manual workarounds exist
- Provide a guide to help “weather the storm”

4 Cyber-Specific Metrics

- Include Recovery Point Objectives (RPOs)
- Evaluate systems

5 Cross-Functional Collaboration

- Encourage tight integration between teams.
- Encourage joint workshops

Examples: Cyber-focused BIA questions

- How will the business operate with manual workarounds?
- Can the manual workarounds be done without IT systems dependencies?
- Do manual workarounds include instructions for recovery after systems are back online?

What are YOU asking your business functions?

- Can these workarounds help the business sustain a 1-week cyber crisis?
- What about an outage of 2 weeks or more?
- Is the responsible team trained?
- Are your services, manufacturing, or products impacted?

Cyber Resiliency Reporting = Actionable Insights

- Does each critical activity have a manual workaround that will sustain the activity for 2+ weeks due to a cyber attack
- Does each application have a manual workaround that will scale for 2+ weeks due to a cyber attack

Establish a Baseline to Improve Upon, Share Results with Leadership

Key Takeaways – There is Power in Alignment!

1. Establish the “Three-Legged Stool” Model
2. Conduct Cyber-Focused Business Impact Analyses (BIAs)
3. Create Joint Incident Response Playbooks
4. Integrate Cyber Risks into the Entire BCP Lifecycle
5. Hold Regular Cross-Functional Drills and Tabletop Exercises
6. Share Metrics and Success Criteria
7. Promote a “Cyber Resilience Mindset” Throughout the Organization

Cross-Team Collaboration Increases Cyber Resiliency

2025 KOnnect

Questions?

CONNECTING RISKS THAT MATTER

Connect with me.

Chris Chaisson, CBCP, CCRP

e: Christopher_Chaisson@amat.com

w: www.appliedmaterials.com

/in/chrischaisson/

2025 KOnnect

2025 KOnnect

CONNECTING RISKS THAT MATTER

THE
MATRIX

Thank You!

CONNECTING RISKS THAT MATTER

2025 KOnnect