FLAIR
DATA SYSTEMS
EST. 1916

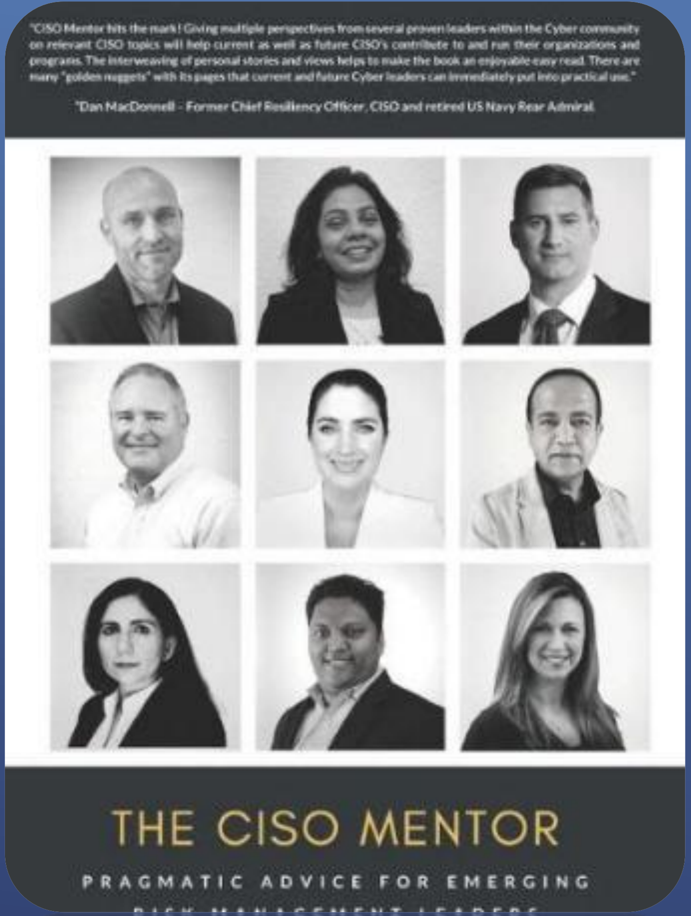
# Focusing on Resiliency in 2026

Moving Beyond Defense to Survive the Inevitable

**Jessica Nemmers**
Field CISO | vCISO

# QUICK INTRO

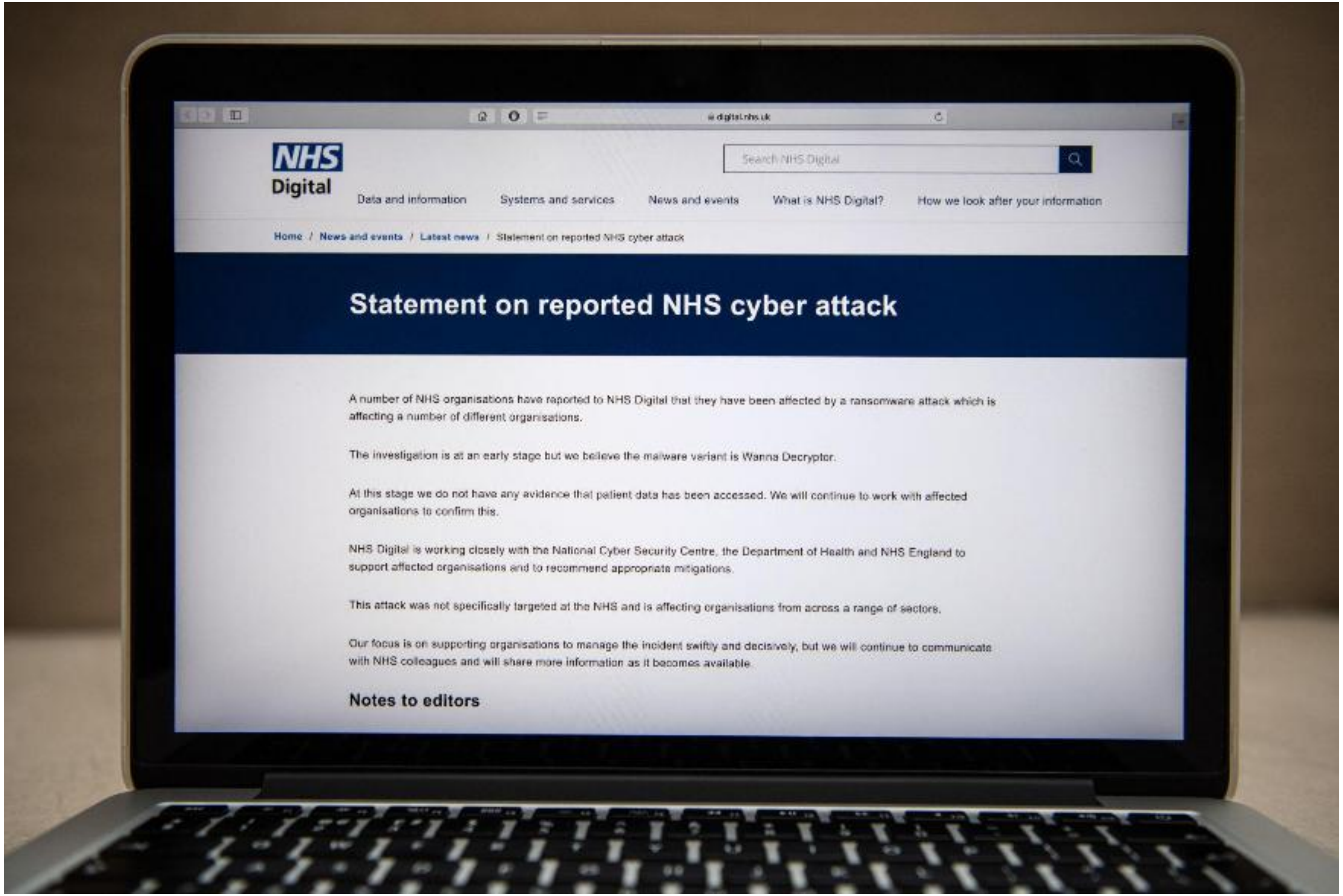
- Flair Data CISO and a vCISO with 30 years in IT and Cybersecurity
- Former Chief Information Security Officer at a Fortune 500 Global Manufacturing Company
- Former Chief Security Officer at a Texas-based Fintech Company
- Recognized by D Magazine as one of the "Top 500 Business Leaders in Dallas"
- Recipient of the "Women in Tech Trailblazer Award" by Dallas Business Journal
- Co-Author of "The CISO Mentor"
- Law enforcement wife and proud mom to four incredible children


"CISO Mentor hits the mark! Giving multiple perspectives from several proven leaders within the Cyber community on relevant CISO topics will help current as well as future CISO's contribute to and run their organizations and programs. The interweaving of personal stories and views helps to make the book an enjoyable easy read. There are many "golden nuggets" with its pages that current and future Cyber leaders can immediately put into practical use."
"Dan MacDonnell - Former Chief Resiliency Officer, CISO and retired US Navy Rear Admiral.
THE CISO MENTOR
PRAGMATIC ADVICE FOR EMERGING
RISK MANAGEMENT LEADERS

# ALSO KNOWN AS THE “BALLERINA TURNED CISO”

Now is the time to shift the cybersecurity conversation from prevention alone to surviving inevitable attacks in an era of AI-driven threats.

This presentation will explore what true resilience looks like in practice and how well-designed Cyber Incident Response, Business Continuity, and Disaster Recovery Plans enable organizations to continue operating when systems, data, and communications are disrupted.



# Statement on reported NHS cyber attack

A number of NHS organisations have reported to NHS Digital that they have been affected by a ransomware attack which is affecting a number of different organisations.

The investigation is at an early stage but we believe the malware variant is Wanna Decryptor.

At this stage we do not have any evidence that patient data has been accessed. We will continue to work with affected organisations to confirm this.

NHS Digital is working closely with the National Cyber Security Centre, the Department of Health and NHS England to support affected organisations and to recommend appropriate mitigations.

This attack was not specifically targeted at the NHS and is affecting organisations from across a range of sectors.

Our focus is on supporting organisations to manage the incident swiftly and decisively, but we will continue to communicate with NHS colleagues and will share more information as it becomes available.

## Notes to editors

# While we were building defenses….

## We weren’t building resilience

# IF YOUR CORE SYSTEM WENT DOWN TOMORROW, HOW LONG WOULD IT BE BEFORE

- Your organization sees financial impact
- Executives are scrambling to protect the company’s reputation
- Safety issues appear
- Customers leave
- The company faces regulatory fines and litigation

# WHAT RESILIENCE ACTUALLY MEANS

**Resilience ≠ Recovery**

**Impact → Stabilize → Continue → Recover**

Business Continuity & Disaster Recovery
BCP
Sustain Operations
Decisions
Manual Operations
Workflows
Communication
DRP
Recover Systems
Backup
Restore
Validate
Go Live
ARE NOT THE SAME

# THREE PILLARS OF RESILIENCE

- Cyber Incident Response Plan (CIRP)
- Business Continuity Plan (BCP)
- Disaster Recovery Plan (DRP)

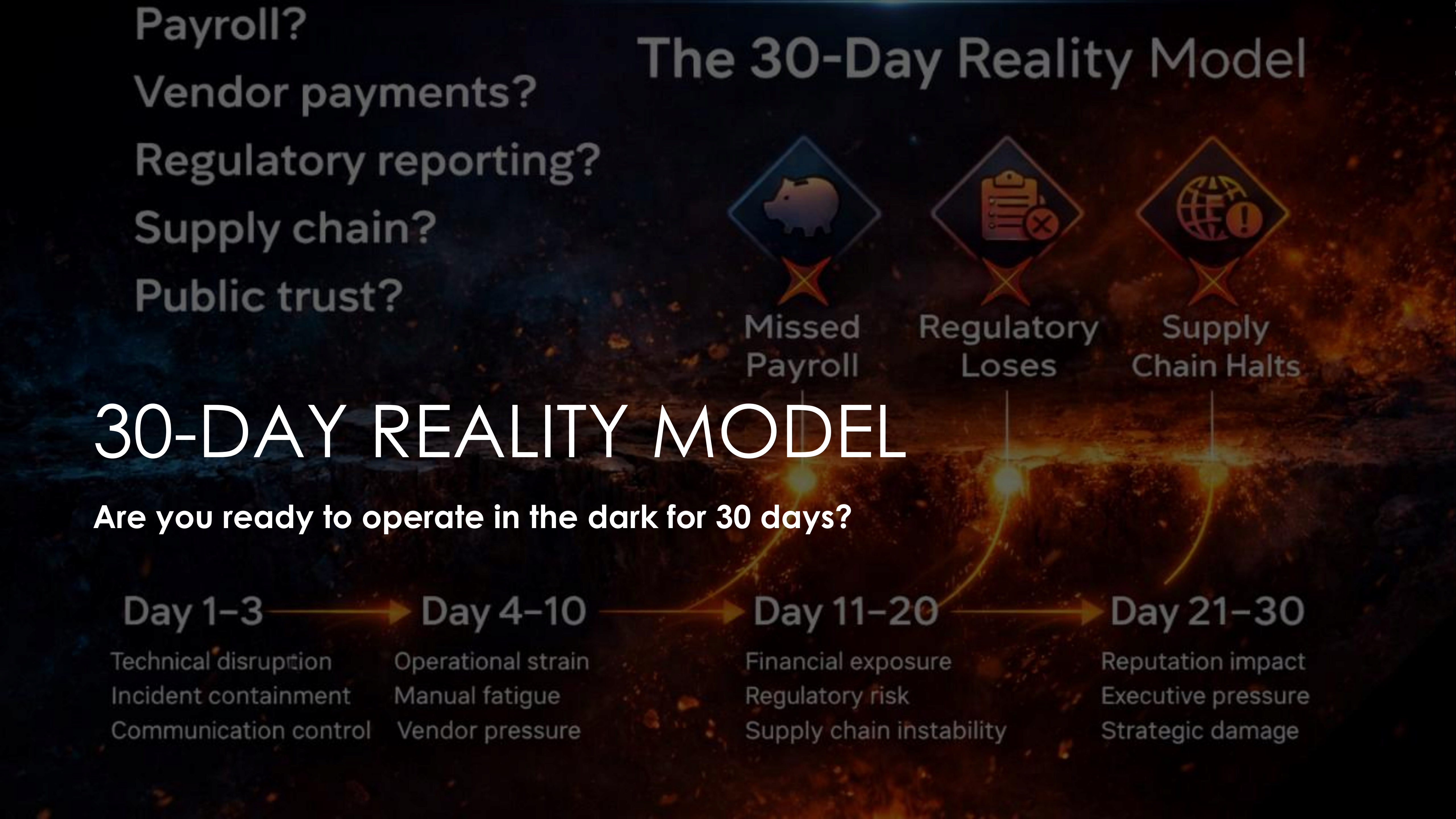
# WHERE MOST PROGRAMS BREAK

Cyber Incident Response Plan (CIRP)
Business Continuity Plan (BCP)
Disaster Recovery Plan (DRP)
THREE PILLARS OF RESILIENCE

- CIRP is written but has not been reviewed or tested
- BCP is written without a Business Impact Analysis (BIA)
- DRP was partially written but no one knows the “Plan”
- There is no training, knowledge or integration of the plans
- DFIR, IT, Security, Communications, Finance, Legal, and HR are all stepping on each other
- Oh…. And the plan is stored in SharePoint, and we can’t access anything

# 30-DAY REALITY MODEL

**Are you ready to operate in the dark for 30 days?**



Payroll?

Vendor payments?

Regulatory reporting?

Supply chain?

Public trust?

## The 30-Day Reality Model

Missed Payroll

Regulatory Loses

Supply Chain Halts

**Day 1–3**
- Technical disruption
- Incident containment
- Communication control

**Day 4–10**
- Operational strain
- Manual fatigue
- Vendor pressure

**Day 11–20**
- Financial exposure
- Regulatory risk
- Supply chain instability

**Day 21–30**
- Reputation impact
- Executive pressure
- Strategic damage

# PLAN 1: THE FIRST 72 HOURS

Cyber Incident Response Plan (CIRP)

- What is the purpose of your Cyber Incident Response Plan?
- Who owns the CIRP?
- Who calls the shots?

Vote with your hands: Is the CIRP a Technical Playbook or a Manual for Executives to Keep Them off the Front Page of the Wall Street Journal?

# CIRP: GOVERNANCE UNDER STRESS

BOTH

# STRUCTURE OF A CIRP

- Roles and Responsibilities
- Confidentiality
- Triggers
- Classification
- Communication
- Playbooks for Triage and Containment
- Expectations for Containment and Eradication activities with the DFIR
- Contact sheets
- After Action Review

**What About Restoration?**

# YOU ARE NOT ALONE

# WHAT ABOUT A DATA BREACH?

- Contain the Threat
- Gather CIRT
- Define/Clarify Roles
- Preserve Evidence
- Define Scope
- Establish Confidential Communication Channels
- Escalate Communications
- Contact the Cyber Insurance Company*
- Document, document, document

# Stabilization

# WHERE CIRPS FAIL

- No specifics on confidentiality
- CIRT and employees are not trained on the plan
- No Incident Manager or Scribe are defined
- Plan is only available online
- Insurance is engaged too early
- No triggers or decision points are planned ahead of time
- No executive communication cadence is defined

# PLAN 2: OPERATING THROUGH THE STORM

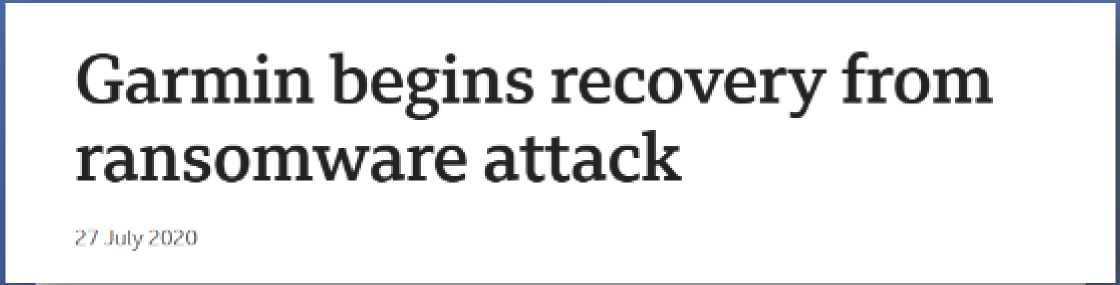
Business
Continuity Plan
(BCP)

# BUSINESS IMPACT ANALYSIS (BIA)

1. What are the most critical functions of the company (top 3)?
2. Why are they the most critical (e.g., patient safety, reputational loss, customer loss, public safety, financial loss, regulatory/compliance requirements)?
3. What technology or systems (don't forget 3rd party solutions) support the most critical functions of the company?
4. How long can you realistically be down before number 2 becomes a big problem?

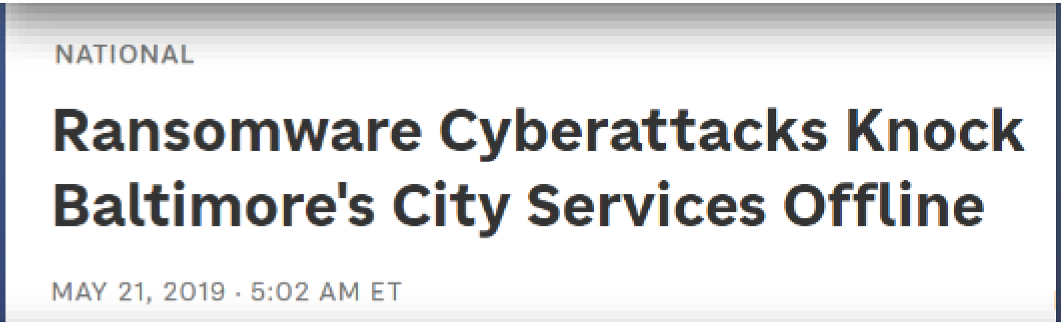
- Roles and Responsibilities
- Formal Initiation of BCP
- Alternate Meeting/Communication Technologies
- Assessed Impact to Critical Functions:
  - Recovery Time Objective: How long before it hurts
  - Recover Point Objective: How much data can we stand to lose
- Communication, Communication, Communication
- Documented Downtime Procedures (Separate Documents/Forms)
- Ongoing Coordination Between Departments, Particularly IT
- Planned Data Integrity Checks
- Formal Declaration to Return to Normal Operations

# STRUCTURE OF A BCP



Garmin begins recovery from ransomware attack

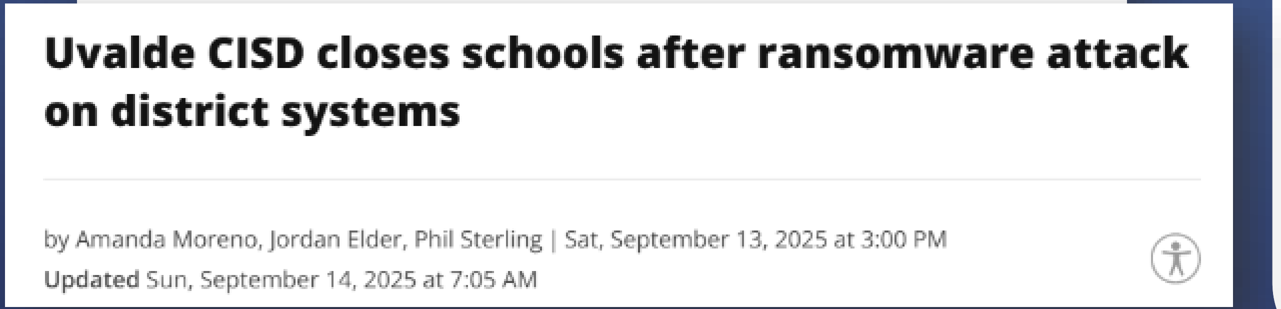
27 July 2020



NATIONAL

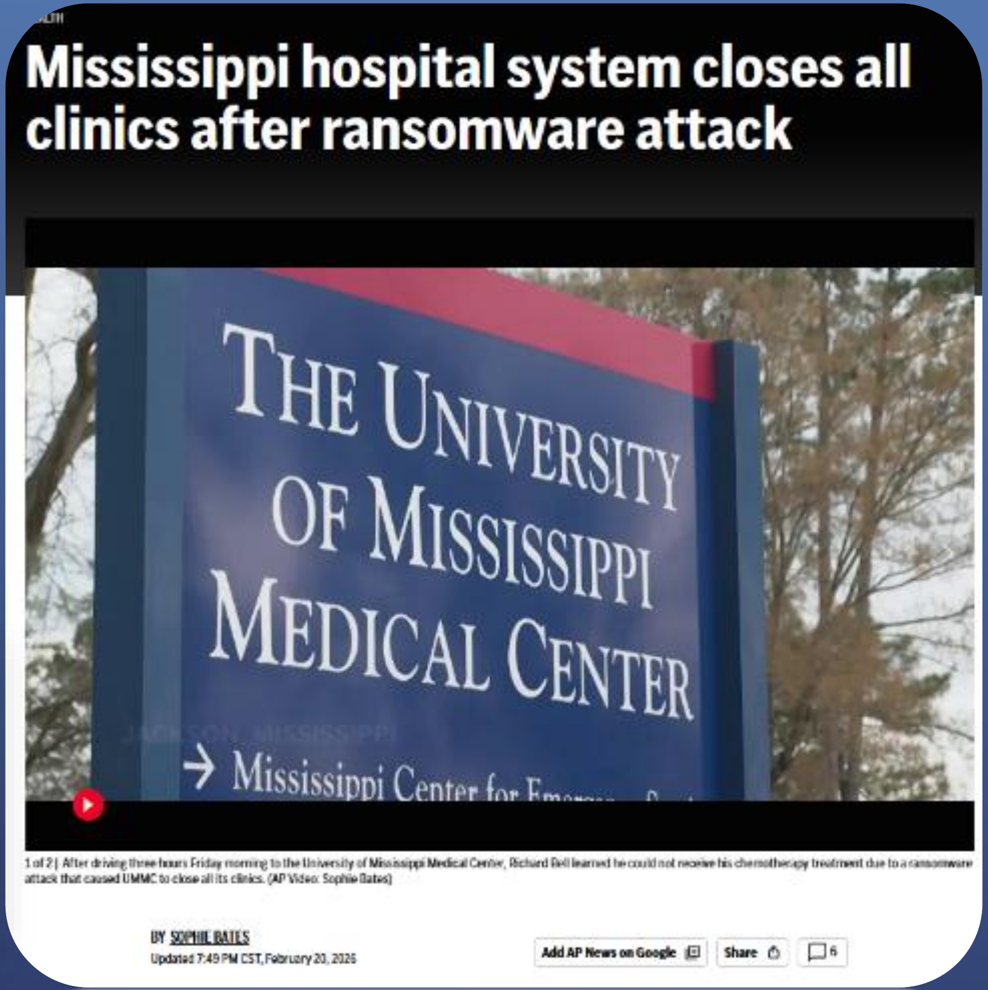
Ransomware Cyberattacks Knock Baltimore's City Services Offline

MAY 21, 2019 · 5:02 AM ET



Uvalde CISD closes schools after ransomware attack on district systems

by Amanda Moreno, Jordan Elder, Phil Sterling | Sat, September 13, 2025 at 3:00 PM
Updated Sun, September 14, 2025 at 7:05 AM



Mississippi hospital system closes all clinics after ransomware attack

THE UNIVERSITY OF MISSISSIPPI MEDICAL CENTER
→ Mississippi Center for Emergency Services

1 of 2 | After driving three hours Friday morning to the University of Mississippi Medical Center, Richard Bell learned he could not receive his chemotherapy treatment due to a ransomware attack that caused UMMC to close all its clinics. (AP Video: Sophie Bates)

BY SOPHIE BATES
Updated 7:49 PM CST, February 20, 2026

ARE YOU READY TO OPERATE BY "PEN AND PAPER?

- Pre-Planned Emergency Preparedness
- Printed Procedures
- Staff Cross-Training
- Alternate Communications
- Defined Communication Escalation Points
- Defined Initiation and Suspension Authority
- Fatigue Planning
- Data Integrity Checks
- Emergency Relocation Site (30-day Operation)

# MANUAL EXECUTION REALITY

# PLAN 3: RESTORING DELIBERATELY

Disaster Recovery Plan (DRP)

# RECOVERY PRIORITIZATION

1. Identity
2. Core
3. Tier 1 Systems, Platforms, Applications
4. Users

- Backup Poisoning
- SaaS Blind Spots
- Cloud Control Plane
- Ransomware in Backups
- Backup Failures

Why? Because backups are not fully protected or tested!

# MODERN DRP RISKS

- Separate Backup Credentials from Primary Identity
- Limit Break-Glass Accounts to two Global Admins
- Implement MFA, PIM, PAM for Privileged Accounts
- Backup SaaS using Third-Party Tools
- Validation through Restore Testing
- Monitor Privileged API Calls
- Log and Alert Management:
    - Logs are being collected
    - Alerts are firing on all potential disruptions that could hinder recovery
    - Logs are stored in immutable storage

# GUARDRAILS TO CONSIDER

# CLEAN ROOM RESTORATION & DFIR PARTNERSHIP

- Validate Eradication/ Ensure No Persistence Remains
- Support Acquisition of Devices and Infrastructure
- Guide Segmented Rebuild
- **Validate Before Connection**
- Documented the Order of Operations

# RTO IN THE REAL WORLD OF RESTORATION

RTO Assumptions:

- Sound Infrastructure
- Backups are Intact
- Identity is Trusted
- No Rebuild, Just Restore

BUT….

- Hypervisors are Compromised
- DCs are Untrusted
- Cloud Tenants Corrupted
- Backups are Poisoned

RTOs Must Consider:

- Hardware Procurement Lead Time
- Firewall Replacement
- Endpoint Reimaging
- Image Validation
- Identity Re-Baselining
- Certificate Reissuance
- Key Rotation
- SaaS Tenant Rebuild

# RTO IN THE REAL WORLD OF RESTORATION

CIRP
Stabilize
DRP
Restore
RESILIENCE
BCP
Operate

# RESILIENCE MATURITY MODEL

- Level 1 – Documented
- Level 2 – Tested
- Level 3 – Executable Offline
- Level 4 – Cross-Functionality Practiced
- Level 5 – 30 Days Survivable

- Conduct or Update BIAs (Departments or Business Units)
- Capture Information in a BIA Report (Identify Strengths and Risks to Resiliency)
- Use the BIA Report to Build the BCP
- Define RTO/RPO Targets with Business and IT Leadership
- Build the DRP with Realistic Scenarios for Tier 0, 1, and 2 Systems
- Run a 30-day Tabletop Exercise
- Align the CIRP, BCP, and DRP with Leadership

# CALL TO ACTION

# PREVENTION IS IMPORTANT

# SURVIVAL IS MANDATORY

Jessica Nemmers

CISO/Field CISO – Flair Data Systems

Jessica.Nemmers@flairdata.com

# THANK YOU!

FLAIR
DATA SYSTEMS
EST. 1916