STONE RISK

WHITEPAPER

LONG-TERM DOWNTIME PREPAREDNESS IN HEALTHCARE

BUILDING RESILIENCE IN THE FACE OF EXTENDED IT DISRUPTIONS

January 2025

WWW.STONERISKCONSULTING.COM

HOSPITALS MUST PLAN NOW FOR INCIDENTS THAT WILL OCCUR

In today's interconnected healthcare environment, IT systems underpin nearly every aspect of hospital operations, from patient records to medication administration.

However, these systems are not infallible. Hospitals face a range of potential disruptions, including cyberattacks, power outages, hardware failures, and natural disasters. When these disruptions occur, they can severely impact the ability to deliver timely and effective patient care.

Recent trends emphasize the urgency of this issue. In 2023 alone, ransomware attacks against healthcare organizations nearly doubled globally, escalating from 214 incidents in 2022 to 389 in 2023.

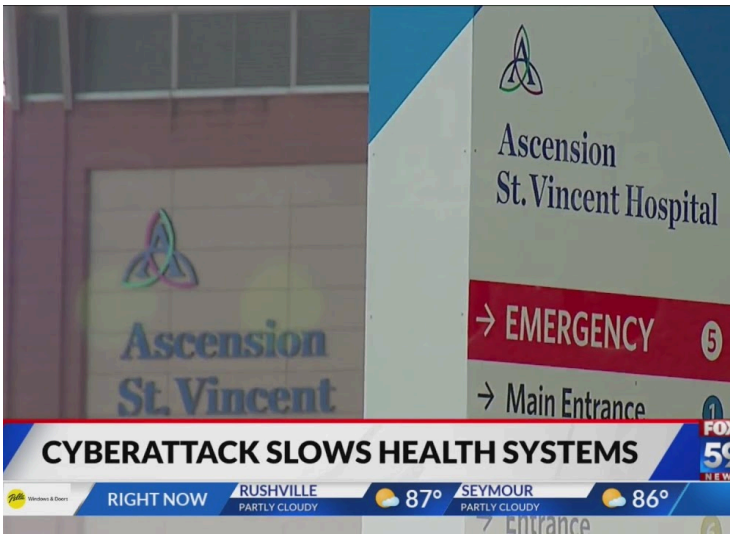
This sharp rise illustrates that the threat landscape is rapidly evolving, leaving hospitals increasingly vulnerable. These attacks have not only increased in frequency but also in impact, with operational disruptions costing U.S. healthcare providers an estimated $21.9 billion in downtime since 2018.

The increasing sophistication and prevalence of these threats make it imperative for hospitals to adopt a proactive approach. Downtime procedures are no longer a contingency measure—they are a core component of operational resilience. By planning now, healthcare organizations can ensure they are prepared to maintain critical workflows and minimize disruptions during inevitable incidents.

Becker's Hospital Review - "Ransomware Costs Healthcare $21.9 Billion in Downtime"
Statista - "Healthcare and Cybersecurity in the U.S."

CASE STUDY: ASCENSION HEALTHCARE'S RANSOMWARE INCIDENT

The June 2024 ransomware attack on Ascension Healthcare serves as a sobering reminder of the consequences of inadequate downtime preparation.



As one of the largest healthcare systems in the United States, Ascension's network encompasses dozens of hospitals and clinics.

When cybercriminals infiltrated their systems, the ensuing outage lasted weeks, disrupting operations across multiple facilities.

The impact on patient care was immediate and far-reaching. Without access to electronic medical records (EMR), clinicians struggled to obtain critical information about patient histories, medication orders, and test results.

Manual processes, hastily implemented, proved cumbersome and error-prone. Delayed treatments and diagnostic errors highlighted the vulnerability of even well-resourced healthcare organizations to IT disruptions.

Operationally, the attack exposed significant weaknesses in Ascension's preparedness. Many departments lacked detailed downtime procedures, relying instead on ad hoc solutions that varied widely in effectiveness. Communication between departments was hindered by the absence of reliable backup systems, compounding the challenges of coordinating care.

Financially, the repercussions were severe. In addition to the ransom demand, Ascension faced millions in lost revenue, increased labor costs, and potential regulatory penalties. The reputational damage further eroded trust among patients and stakeholders, demonstrating the long-term risks associated with insufficient planning.

NPR - "Ascension Hospital Ransomware Attack and Care Lapses"

HOSPITALS MUST MAKE PROVISIONS FOR PLANNED, UNPLANNED, AND LONG-TERM DOWNTIME

Healthcare facilities routinely schedule **planned downtimes** for routine system maintenance, software updates, or infrastructure upgrades.

These events, while temporarily inconvenient, are predictable and allow for careful preparation, minimizing their impact on operations.

In contrast, **unplanned downtimes**—caused by cyberattacks, power failures, or natural disasters—present a more complex challenge, often catching organizations off guard.

Yet, even more disruptive are **long-term downtimes**: extended outages that last days, weeks, or even longer, pushing hospital systems and staff to their limits.

Long-Term Downtime: Preparing for the Unthinkable

Long-term downtimes are a growing concern, driven by the increasing frequency of severe ransomware attacks and infrastructure failures. Unlike short-term disruptions lasting a few hours, long-term downtimes can extend over days or weeks, compounding challenges for hospitals ill-equipped for prolonged outages.

These events require:

- **Sustained Workflow Adaptations:** Hospitals must implement manual processes for critical workflows such as medication administration, diagnostic services, and patient tracking. These processes must be efficient enough to sustain operations over extended periods.
- **Resource Management:** Extended outages strain supplies, including paper forms, backup power sources, and communication tools. Proactive stockpiling and resource allocation plans are essential.
- **Enhanced Staff Resilience:** Long-term downtimes place significant psychological and physical stress on healthcare workers. Comprehensive training and support systems help staff navigate the prolonged demands of manual workflows and alternative procedures.
- **Coordination Across Departments:** Hospitals must foster interdepartmental collaboration to maintain seamless operations despite the absence of digital systems. This involves synchronizing efforts across clinical teams, IT, and administrative staff.

BEST PRACTICES FOR LONG-TERM DOWNTIMES

At Stone Risk Consulting, we have worked extensively withing hospitals and healthcare organizations to prepare for the challenges posed by long-term IT system outages.

Through these experiences, we have uncovered common vulnerabilities and identified actionable strategies to mitigate the impact of disruptions.

Our experience highlights that while many hospitals prioritize their electronic medical record (EMR) systems, they often overlook the critical dependencies and workflows that sustain seamless operations across the organization.

Long-term outages, whether caused by cyberattacks, natural disasters, or system failures, expose weaknesses in communication, resource allocation, and manual workflow readiness.

These challenges demand a proactive, organization-wide approach to ensure patient care remains uninterrupted and operational continuity is maintained.

The following best practices, derived from our consultancy's fieldwork and findings, provide a roadmap for building resilience against IT disruptions.

1 Formalizing Activation Criteria

One of the most pressing challenges hospitals face is determining when to activate downtime procedures.

Clear activation criteria are essential to ensure timely and coordinated responses to events like ransomware attacks or system failures. Effective coordination relies on predefined roles and responsibilities, enabling staff to respond decisively and minimize delays.

2 Developing Downtime Procedures for Critical Communication Systems

Communication breakdowns are a recurring issue during IT outages. Hospitals depend heavily on digital communication systems, which can become inaccessible during disruptions.

Alternative communication methods, such as phone trees, secure radios, and physical check-ins, must be established to ensure the flow of critical information, including patient updates and emergency alerts.

3 Identifying Critical Services to Curtail or Modify

Not all hospital services can operate at full capacity during a prolonged IT outage. Identifying which services are essential to patient care and which can be temporarily curtailed allows hospitals to allocate resources effectively.

For example, elective procedures might be postponed to prioritize emergency care and critical patient workflows.

4 Develop Downtime Procedures for Shared IT Systems and Equipment

Shared IT systems and medical equipment, such as diagnostic imaging platforms, medication dispensing tools, and laboratory systems, often have interdependencies that amplify the impact of outages.

Hospitals must develop detailed, department-specific procedures to ensure these critical tasks can continue through manual workflows or alternative processes.

5 Simplifying Templates, Tools, and Documentation

The complexity of hospital operations necessitates user-friendly tools and documentation. Simplified templates, checklists, and manuals help staff adapt quickly to manual workflows.

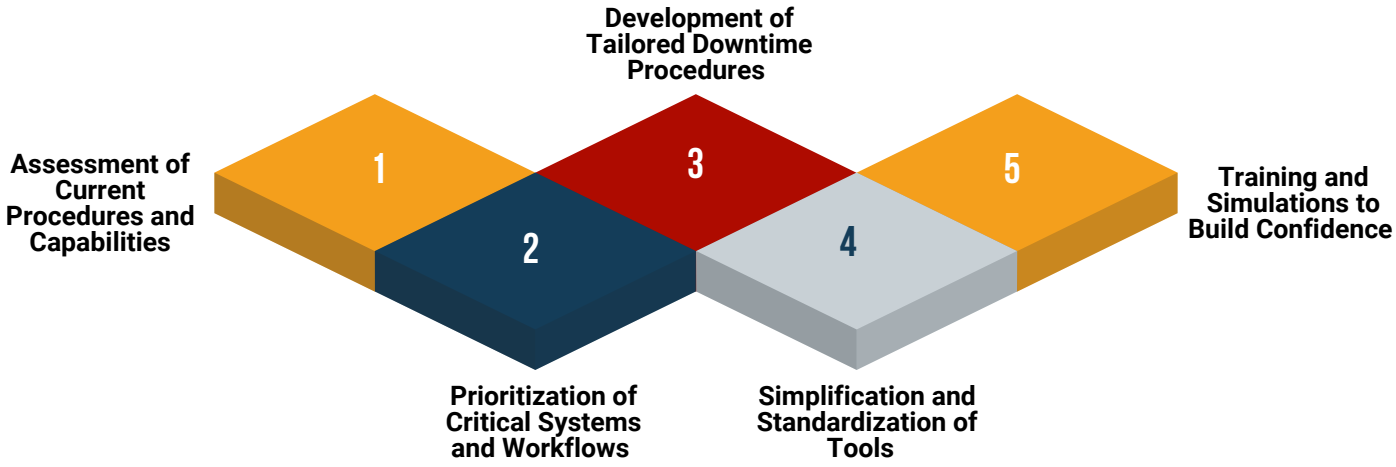
By reducing confusion and cognitive load, these resources enable teams to maintain operational efficiency and focus on patient care during high-pressure scenarios.

6 Enhancing Preparedness Through Training and Simulations

Hospitals must incorporate regular training and simulation exercises into their preparedness plans. These drills replicate the conditions of a long-term IT outage, allowing staff to practice manual workflows, test communication protocols, and identify procedural gaps.

Ongoing training ensures that staff are confident and capable of executing downtime procedures effectively.

LONG TERM DOWNTIME PREPAREDNESS ENGAGEMENT OVERVIEW



At **Stone Risk Consulting**, we recognize that preparing for downtime requires more than generic protocols—it demands a tailored, strategic approach that addresses the unique challenges and dependencies of each healthcare organization.

Our Recommended Approach to **Long-Term Downtime Preparedness** is built on our extensive collaboration with hospitals and health systems.

This overview outlines the key components of our engagement which will equip your organization to manage both planned and unplanned IT disruptions with confidence.

1 Assessment of Current Procedures and Capabilities

We begin by conducting a detailed evaluation of your hospital's existing downtime procedures. This includes:

- **Documentation Review:** Analyzing existing plans, policies, and protocols to identify gaps and redundancies.
- **Stakeholder Input:** Engaging clinical, administrative, and IT teams to understand pain points and real-world challenges.
- **Workflow Mapping:** Examining critical workflows across departments to identify dependencies on IT systems and medical equipment.

This phase helps establish a baseline, revealing areas that require immediate attention and opportunities for improvement.

2 Prioritization of Critical Systems and Workflows

Not all systems and workflows are equally critical. Our approach focuses on identifying and prioritizing the ones essential to patient care and operational continuity. This involves:

- **Ranking systems by their impact** on patient safety and care delivery.

- **Highlighting workflows** that span multiple departments, such as medication administration, diagnostic imaging, and patient admissions.
- Determining which **services can be curtailed** or modified during extended outages to allocate resources effectively.

This prioritization ensures that efforts are directed where they are needed most.

3 Development of Tailored Downtime Procedures

Using insights from the assessment, we collaborate with your team to create downtime procedures tailored to your organization's unique needs. Key elements include:

- **Activation Criteria and Triggers:** Establishing clear thresholds for initiating downtime protocols.
- **Alternative Workflows:** Designing manual processes to replace digital systems during outages.
- **Communication Plans:** Ensuring effective interdepartmental and external communication using backup methods.

Our tailored procedures address the specific challenges your hospital faces, ensuring readiness for both planned and unplanned disruptions.

4 Simplification and Standardization of Tools and Documentation

To facilitate adoption and usability, we create user-friendly tools and resources that empower your team during an outage:

- **Customized templates** for workflows, logs, and checklists.
- **Centralized guides** that consolidate critical information into an accessible format.
- **Standardized procedures** across departments to eliminate inconsistencies.

This approach simplifies implementation, ensuring staff can easily execute procedures under high-pressure conditions.

5 Training and Simulations to Build Confidence

Preparedness requires practice. We develop and deliver training programs and simulation exercises that:

- **Familiarize staff** with downtime procedures and manual workflows.
- **Test the organization's response** to realistic outage scenarios.
- **Identify gaps** and opportunities for refinement through hands-on experience.

TAKE THE FIRST STEP TOWARD DOWNTIME PREPAREDNESS

At **Stone Risk Consulting**, we specialize in helping healthcare organizations build resilience against IT disruptions.

Our tailored solutions empower hospitals to navigate the complexities of planned and unplanned outages, ensuring continuity of care and operational efficiency.

Whether you're addressing gaps in your existing downtime procedures, preparing for cybersecurity threats, or aiming to strengthen your organization's overall resilience, we're here to help.

Together, we can craft a comprehensive strategy that meets your unique needs and secures the future of your operations.

What You'll Gain:

- **Actionable insights** into your organization's vulnerabilities and priorities.
- **Customized downtime procedures** aligned with your critical workflows.
- Tools and templates that simplify implementation and empower your team.
- **Confidence in your preparedness** through hands-on training and simulations.

Let's Get Started

Learn more about our *Long-Term Downtime Preparedness* engagements and how **Stone Risk Consulting** can support your journey toward preparedness.

CONTACT US TODAY:

Visit our Website:
stoneriskconsulting.com

Schedule a Consultation:
www.stoneriskconsulting.com/contactus