THE EVOLVING IMPORTANCE OF HEALTHCARE RESILIENCY

PREPARING YOUR HOSPITAL FOR A CRISIS

IMEG

INTRODUCTION:

What is Healthcare Resiliency and Why is it Important?

When disaster strikes, hospitals and healthcare systems are on the front line of ensuring community safety and resiliency.

However, this purpose can only be served if your hospital is prepared to face the worst. By taking proactive steps and making concrete plans to further the disaster preparedness of your healthcare facility, you'll be better equipped to answer the call of your community during dire situations.

In addition to being resilient to natural disasters, hospitals also cannot allow other disruptions such as power outages, water shortages or infrastructure failures to impair their ability to provide lifesaving care to their vulnerable patient population. Without a clear plan and definitive course of action in place ahead of time, your hospital could be left scrambling to recover, putting patients and staff at risk and leaving your facility liable.

The Evolution of Healthcare Resiliency

Establishing a disaster-resilient healthcare institution is becoming an exceedingly more complex problem. Even hospitals that feel confident in the resiliency of their building and their contingency plans may find gaps and inconsistencies with the reality of today's changing world. Natural disasters like the 2011 tornado in Joplin, Mo., the wildfires in California and the flooding from Hurricane Sandy in 2012 have always been a risk. However, due to our changing planet, the frequency and severity of these events is increasing.

Beyond natural disasters, hospitals also need to plan for how they would respond to other physical threats, like active shooters or mass casualty events. There is also the potential for unforeseen risks, such as infectious disease outbreaks that could cripple a region and induce panic, or the risk of a cyber-attack, which could lead to financial loss or breach in patient privacy.

With such a broad range of threats that can occur, how can you ensure your hospital is adequately prepared? Further, assuming the requirements for healthcare resiliency will continue to evolve, how can you ensure your hospital stays adequately prepared?

Answering these questions first requires an understanding of four commonly accepted characteristics of infrastructure resiliency, as defined in 2009 by the **NATIONAL INFRASTRUCTURE ADVISORY COUNCIL:**

- **Robustness:** the ability to maintain critical operations and functions in the face of crisis. This includes the building itself, the design of the infrastructure (office buildings, power generation, distribution structures, bridges, dams, levees), or in system redundancy and substitution (transportation, power grid, communications networks).
- **Resourcefulness:** the ability to skillfully prepare for, respond to, and manage a crisis or disruption as it unfolds. This includes identifying courses of action and business continuity planning, training, supply chain management, prioritizing actions to control and mitigate damage, and effectively communicating decisions.
- **Rapid Recoverys:** the ability to return to or reconstitute normal operations as quickly and efficiently as possible after a disruption. Components of rapid recovery include carefully drafted contingency plans, competent emergency operations, and the means to get the right people and resources to the right place.
- **Redundancy:** having back-up resources to support the originals in case of failure.

Using these traits as a benchmark, you can begin to take an informed look at the main resiliency issues facing your healthcare facility. You can then conduct a thorough vulnerability assessment to discover ways your building and operations may fall short. The vulnerability assessment can be very broad or threat specific, but it is critical the assessment be thorough, as well as include key team members within the health system and third party experts as required.

5 Key Areas of Healthcare Resiliency

According to the **NATIONAL INSTITUTE OF BUILDING SCIENCES,** "Resilience is multidisciplinary and needs the cooperation of different disciplines for successful outcome. Without multidisciplinary cooperation and contributions, there cannot be successful or efficient resilient infrastructure."

This guide will take a broad, multidisciplinary look at five key areas of healthcare resiliency, and the considerations you'll need to make for each to ensure your institution is ready to survive a crisis. Each of these areas are complex and will require much more detailed expertise in order to achieve true resiliency, but our purpose is to deliver a broad overview of the following:

Chapter 1: Natural Disasters and the Structural Integrity of Your Hospital

Chapter 2: The Effect of Disaster on Your Hospital's MEP Infrastructure

Chapter 3: Hospital Physical Security — Beyond Guards and Cameras

Chapter 4: Reacting to Mass Casualty Events or Infection Outbreaks

Chapter 5: Protecting Your Hospital From Cyber Security Vulnerabilities

Bonus: Healthcare Resiliency Preparation Checklist

These key areas represent many of the overlooked and misunderstood aspects of hospital risk management. By using this guide as a starting point to thoroughly consider each area within your institution, you can ensure your hospital is better prepared to handle a crisis — regardless of which type comes your way.

CHAPTER 1

Natural Disasters and the Structural Integrity of Your Hospital

Natural disasters may be unstoppable, but that doesn't mean your hospital can't take intentional and necessary steps to lessen their impact.

While the specific natural disasters you should be concerned about — and many of the specific actions you should take in response — depend on your geographic location, there's no such thing as being too prepared.

You're likely already familiar with the big categories of natural disasters: tornados, hurricanes, floods, wild fires, and earthquakes. Beyond these significant events, there are other weather- and terrain-related events — such as heat waves, mudslides, avalanches and tsunamis — that are considerably less common or impactful. The structural and architectural design of your building doesn't necessarily need to take every potential natural disaster into account, but it should consider common events for your area, as well as potentially devastating, but unlikely chance occurrences, such as fire.

Beyond establishing procedures and educating your staff on hospital policies in the event

of a natural disaster, here are several factors about your hospital structure that you'll need to consider.

3 Structural Questions to Prepare Your Hospital for a Natural Disaster

1. DO YOU WANT YOUR HOSPITAL TO BE A COMMUNITY BEACON?

In times of great tragedy or upheaval, communities often turn to hospitals to act as a gathering place or safe landing amidst the chaos. It is not uncommon for people with nowhere else to go during a disaster to go to a hospital, even if they don't need medical care. Assuming your hospital makes it through whatever disaster befalls your community, you'll need to consider whether you want your hospital to become a community beacon.

If the answer is yes, you'll also need to put in place procedures to ensure your hospital is prepared to take on this role. First and foremost is the designation of a disaster response area — ideally one that is hardened against potential disaster effects and prepared to take on an influx of people.

2. DOES THE PHYSICAL DESIGN OF YOUR BUILDING POSE ANY CHALLENGES?

Consider how the layout of your building would function in a disaster. For instance, are your emergency generators or back-up fuel pumps in the basement? This could leave your hospital without these critical systems in the event of a power outage if your basement experiences flooding. Or, consider the locations of the emergency exit stairwells in your building. Ideally, they should discharge into remote areas of your hospital that aren't high risk for damage or physical attack. In order to create safe fire exits, stairways should also be maintained with positive pressure from a clean source of air, which will help keep smoke and toxic fumes out.

Since there are numerous variables in the physical design of your building that could become hazardous during a natural disaster, the safest and most thorough course of action is to conduct a full building vulnerabilities assessment with a professional.

3. IS THE HARDNESS OF YOUR BUILDING PREPARED TO HANDLE ADVERSE CONDITIONS?

During a natural disaster, your building could be subjected to high winds and substantial rains. By hardening your building to take on these outside forces, you can ensure critical areas remain safe and minimize damage, allowing your hospital functions to continue. While building codes require your building be able to withstand a certain wind level, further hardening may be necessary if hurricanes and tornados are common in your area.

For example, the Van Diest Medical Center, in Webster City, Iowa, constructed a 1,500-square-foot storm shelter area to provide a designated area of protection to keep people safe for a

short period of time during a catastrophic event. Designed for 250 mph wind pressure and impact force from a FEMA-defined projectile, the space has precast concrete walls, a precast concrete hollow core roof with three inches of concrete topping, no exterior windows, and projectile protection detailing for all vulnerable systems. The newly constructed area serves a dual purpose with the radiology program but allows the hospital to avoid making special construction accommodations to the entire building.text

Summary: While many hospitals wait until it is too late to make structural changes designed to improve resiliency, there's no such thing as being too prepared. Preemptively improving the resiliency of your hospital through architectural and structural changes can make all the difference in your facility's ability to withstand a disaster.

CHAPTER 2

The Effect of Disaster on Your Hospital's MEP Infrastructure

Maintaining the inner workings of your hospital's vital systems is also crucial to the continuing operation of your building during a natural disaster.

The mechanical, electrical, and plumbing (MEP) infrastructure of your facility needs to be sufficiently protected and hardened against potential events in order to remain operational in a crisis. Without adequate power, ventilation, and water, your hospital will quickly lose its ability to provide service and safety to patients and staff.

So, how can you increase the resiliency of your hospital's MEP infrastructure?

First, determine what level of continuity your systems will need to maintain in the event of a disaster. Next, consider the types of threats your systems may encounter and what vulnerabilities they would face against those threats. While your best course of action is to bring in an MEP engineer to thoroughly assess your facility's risks and gaps, we've outlined the following five risk areas and concerns as a starting point.

5 Key Considerations to Increase Resiliency in Your MEP Infrastructure

LOCATION OF BUILDING SYSTEM EQUIPMENT

As mentioned in Chapter 1, it's not uncommon for facilities to have electrical equipment and emergency power infrastructure located in the lower level. While it might initially seem to be a good idea to have these systems in non-premium space, locating them in the lowest level of a building increases the risk of flood damage. This is especially dangerous if your hospital is located in a floodplain or your building is at or below sea level. During the planning stages, one of the simplest steps you can take to reduce the risk of flooding affecting your MEP systems is to locate critical equipment on higher levels. For example, the generators at Memorial Medical Center in uptown New Orleans were able to withstand the initial impact of Hurricane Katrina in 2005, but the flooding in the following days reached the emergency power transfer switches, expediting the evacuation of the facility.

HARDNESS OF SYSTEMS

Hardness refers to the process of reinforcing individual systems within your hospital to make them more resilient against disaster. For example, during the planning stages of the Advocate Aurora Summit Hospital in Wisconsin, it was decided to locate the central utility plant 500 feet away from the hospital, connected with a utility tunnel. One of the main drivers for segregating the central utility plant from the main hospital was to hedge against a disaster potentially impacting both locations simultaneously. The remote plant also allowed for the space to house underground fuel storage to allow the generators to run for 96 hours. By hardening their utilities, the replacement building will be far more prepared if and when disaster strikes.

REDUNDANCY

Baseline redundancy for critical infrastructure items such as boilers, medical gas, and power are required by code for healthcare facilities, but additional redundancy should be a key consideration when evaluating the resiliency of your MEP systems. For instance, assume your building load is 1,000 tons of cooling and you have two 500-ton chillers. If one chiller breaks down or is compromised, your facility will only have 50 percent of the required cooling capacity available. To safeguard against this potential problem, you could plan for one of the following:

- Purchase a back-up 500-ton chiller to have on hand in case of emergencies
- Have three 500-ton chillers to have an N+1 capacity, or, in other words, 100 percent back up available should a single chiller fail
- Upsize both of your chillers to be 750-tons, so you'll still have 75 percent of what you need if one fails
- Install outside piping to bring in an emergency back-up chiller when needed

Though this example is specific to water chillers, the same logic can be applied to other major infrastructure such as emergency generators, air handling units, or critical distribution pumps. Consider this: what would happen if your boiler went down? Not only is a hospital boiler essential to providing heat for employees and patients, it's also important to heat water and sterilize critical equipment. Having a back-up boiler ensures that this functionality is not lost if something happens to your main boiler. Ideally, your main boiler and your back-up boiler would be connected on the same network, so the back-up could immediately begin working after the main boiler fails, thus leaving no gaps in service.

The importance of having redundancies and back-up plans can be applied to all necessary systems and processes in your hospital. For

instance, consider your plumbing system. What would you do if you could no longer flush toilets? That leads us to our next consideration: potable water.

POTABLE WATER

Other than pallets of bottled water, it's rare for hospitals to store water. This can lead to significant problems if something interrupts your water supply. How will you flush toilets? Wash and sterilize equipment? How much drinking water will you need over a fixed period of time?

To answer these questions, first determine how much water usage you truly have at your facility. A week's worth of water might not be as much as you think. Once you understand your usage, you can make an informed decision of how much water you'll need access to in an emergency. While on-site water storage is the best solution to this potential problem, you can also contract out to a pumper truck to be available in emergency situations.

Beyond making a plan for access to water in case of emergency, you can also enact procedures to save and reuse water. Plan to shut off water to designated, non-essential areas of the hospital, use recycled water to flush toilets, or install a roof drain for condensation recovery.

Summary: The process for making your MEP infrastructure more resilient involves careful thinking and consideration of your hospital's specific functions and needs. By addressing vulnerabilities in your systems ahead of time, you can avoid the challenges and tragedies that can occur when hospitals get caught unprepared.

CHAPTER 3

Hospital Physical Security — Beyond Guards and Cameras

By their very nature, hospitals should be safe places. Yet, despite the amount of healing that occurs within the walls of a hospital, the physical security of the building is often at high risk.

There are a few key reasons why hospitals are vulnerable to physical dangers. Since they are open all the time and accessible to the public, potential intruders can gain easy entrance. Plus, patients and family members often experience stressful or traumatic experiences within hospital walls, which can heighten emotions and reactions. In fact, workers in a healthcare setting are **FOUR TIMES MORE LIKELY TO BE VICTIMS OF WORKPLACE VIOLENCE** than private industry workers.

Considering these factors, the physical security of your hospital is clearly an important piece in healthcare resiliency. Yet, safeguarding your hospital from a malicious intruder or physical attack requires more than basic security measures like guards and cameras — and it all starts with restricting and controlling access to your building.

One of the most effective ways to increase the physical security of your hospital without creating an overly institutionalized aesthetic is by leveraging architectural elements to create secure environments. These strategies are called Crime Prevention Through Environmental Design (CPTED) principles, and here's how

you can incorporate them — as well as other strategies — in your exterior and hospital entrance design.

Restrict the access points to the building

Ideally, you want your hospital to have designated, specific entrances for public access. This allows for easier monitoring, and gives you the option to set up secure visitor screening. Utilizing vegetation and various architectural elements can help drive people away from entrances you don't want them to use and toward your main entrance.

While you need to have numerous egress doors to be up to code, there are steps you can take to ensure your emergency exits are only used in the case of an emergency. With proper signage, alarms, camera monitoring, and even removing the entrance-side door hardware, you can better control which doors permit entry into your hospital.

Separate visitor and employee parking lots

One of the biggest physical security concerns every hospital should have is for their staff. To limit the potential for interactions with angry patients or disgruntled family members, keep public access points separate from employee access points. By establishing a perimeter boundary for an employee parking lot, you can create a level of protection within the parking area so staff can move back and forth to their vehicles safely.

Utilize effective parking lot lighting

More than brightly lit parking lots, you need evenly lit parking lots. When lighting is too bright in some areas, it can have the effect of making other areas seem darker. Instead of using really big, bright lights, aim for more frequent lights that have a high level of distribution over your parking lots. This can play a significant role in security by increasing visibility and improving camera coverage.

Create vehicular boundaries

Pedestrian traffic needs to be protected from vehicular traffic, and creating a clear separation between the two can minimize incidents. For instance, more than just a crosswalk, consider using pavement changes, lighting changes, and rumble strips to draw attention to the separation. You can also use CPTED principles to restrict vehicle access to buildings through bollards and curbing. Just ensure the restrictive elements you're using have practical stopping power, rather than just aesthetic appeal.

Limit access to ambulance delivery areas

Separating the ambulance delivery area from the public emergency entrance will limit confusion and ensure an intruder isn't gaining access to your hospital through a vulnerable and often chaotic area. This can be as simple as creating an environment that the public won't be drawn to or isn't readily visible from the front of your hospital, which can be done with additional vegetation or barriers.

Consider how you will handle after-hours traffic

It's not uncommon for hospitals to have all after-hours traffic enter through the Emergency Department. While this is a fine solution, it's still important to consider what this policy does to your parking access. How far away from that entrance are people going to have to park? What kind of exposure will they have while walking to and from their car? In order to make this a safe option, you may need to consider additional lighting and protective barriers.

Utilize glass vestibules as boundaries for secure entry

The entrance to your hospital should be warm and welcoming — but it also needs to be safe. Luckily, you can increase the security by creating a glass vestibule to act as an additional set of doors necessary to gain entry. Depending on the location of your hospital and your risk for gun violence, you could consider making the entrance glass bulletproof. At minimum, it should be laminated glass so it won't immediately shatter if hit.

Make emergency departments escapable

Admitting and waiting areas in emergency departments are often high stress spaces in which tempers can flare. To protect your employees working in these areas, create safe points and escapable options in case they feel threatened. For instance, while a desk can act as an initial boundary, having an additional exit behind the desk through which the employee can slip out if threatened adds an extra layer of protection.

Summary: While physical security at hospitals is often focused on guards and cameras, the design and accessibility of your building can be just as significant in preventing intrusion and outside dangers. By employing CPTED principles and other strategies to limit access, you can more effectively control the physical threats your hospital faces and increase your resiliency in the face of violence.

CHAPTER 4

Reacting to Mass Casualty Events or Infection Outbreaks

When a mass casualty event hits your community or a highly contagious infection breaks out, your hospital will need to be prepared to contain the situation and minimize damages.

Both of these types of occurrences are clearly out of the normal operations of your hospital — but healthcare resiliency is all about preparing your facility to deal with the abnormal.

How your hospital reacts in the minutes and hours after a mass casualty event or infection outbreak can be the difference between lives saved and lives lost. Having procedures and plans in place for quick action is essential to achieving resiliency. The specific courses of action will depend largely on your hospital's capabilities and unique situation, but here are a few broad questions you'll need to answer as you develop your plans.

4 Questions to Ask When Preparing for a Mass Casualty Event

HOW WILL YOU TRANSPORT PATIENTS IF YOU REACH CAPACITY?

The October 2017 shooting in Las Vegas left hundreds of victims in need of emergency surgery. Since the hospital couldn't possibly handle every surgery on site, they had to have a plan for how to transport patients to different

facilities to get the care they needed. Consider how your hospital would react if you reached capacity and were unable to service a large, critically-injured population.

DO YOU HAVE THE INFRASTRUCTURE TO EXPAND YOUR ED QUICKLY?

Your Emergency Department is designed to handle a daily influx of patients — not a mass casualty event. However, you can make adjustments to your building's infrastructure to expand your services quickly if the need arises. For instance, you can hide medical gas outlets and oxygen vacuums in the corridor to expand service locations and increase the number of patients you can treat. With specific artwork systems that can cover these outlets, you won't even know they're there until you need them.

HOW WILL YOU HANDLE EXTRA EMERGENCY RESPONSE VEHICLES?

If multiple emergency response vehicles will be descending on your hospital at once, you'll likely need a designated space to direct them to park. Additionally, since most hospitals only have one helipad, consider if there is a way to set up an additional temporary helipad. This can be as simple as putting pavers down in a grassy area.

DO YOU HAVE A PLAN TO CONTROL FAMILY MEMBERS AND MEDIA?

A mass casualty event is newsworthy and nerve-wracking. When one occurs, your hospital will likely be surrounded with media looking for the story and family members hoping their loved ones are safe. You'll need a strategy to manage this crowd and ensure they can get enough information to calm the panic.

3 Questions to Ask When Faced With an Infection Outbreak

WHAT IS YOUR PROTOCOL FOR QUARANTINING A PATIENT WITH AN INFECTIOUS DISEASE?

When you discover a patient has a highly infectious disease — like Ebola — you need to act quickly to ensure the least amount of exposure. That's why you need a clearly established protocol that all relevant staff are aware of and have adequate training to execute.

DO YOU HAVE A PERMANENT OR TEMPORARY QUARANTINE SPACE?

Most hospitals don't support a permanent quarantine space since it can be a substantial investment to create a space that is used rarely, if ever. For this reason, the most popular option is to have an adaptable space that can be quickly assembled when necessary. You'll need to consider where to put this adaptable space in relation to your HVAC system so you can maintain the right pressure for sterility.

Summary: Mass casualty events or infection outbreaks are often full of panic and misinformation. Failing to plan for these rare but potentially deadly events could leave your hospital ill-equipped and liable, resulting in sub-par patient care. By ensuring you are as prepared as possible to address these circumstances, you can minimize their effects.

CHAPTER 5

Protecting Your Hospital From Cyber Security Vulnerabilities

We've covered several different types of disasters that can threaten the resiliency of your healthcare facility — from natural disasters, to physical intruders, to highly infectious diseases. Yet, there's another significant threat that all modern hospitals need to be conscious of: cyber-attack.

Without thoroughly protected cyber security, you leave your hospital's cyber infrastructure vulnerable to a malicious breech. And it's not just outgoing hacking attacks that you need to worry about — threats can come from both inside and outside your network. For instance, intrusions can be introduced inside your network from an infected USB flash drive or through a vendor unknowingly creating an unprotected connection to the outside world.

The purpose of a healthcare cyber-attack is likely to be for one of two reasons:

1. Accessing electronic hea lth records to sell on the black market.
2. Using ransomware to hijack systems and prevent access until a ransom is paid

Both types of attacks can be devastating for your hospital's reputation and ability to continue to function. Unfortunately, creating a secure cyber network in today's hyper-connected world is a bigger challenge than many hospital IT departments realize.

The "Internet of Buildings" and Lesser-Known Vulnerabilities

You're likely familiar with the term the "Internet of Things," or IoT. This refers to all the daily devices and everyday objects we use that are now enabled with network connectivity. Objects that formerly were not connected to the network — like appliances, automobiles, light switches, and televisions — now are all connected, creating the Internet of Things. The premise behind the IoT is that all of these devices and objects are collecting and sharing data. This massive aggregation of data ("Big Data") can be automatically analyzed by computer algorithms ("artificial intelligence") to determine identifiable patterns that can eventually be leveraged for more efficient, effective use of the individual objects and systems.

That same concept can be applied specifically to your hospital building through what we have termed the "Internet of Buildings," or IoB. More than any other building type, hospitals have a significant number of potential smart devices, building systems, clinical equipment, and other leading-edge technology that can be connected, providing countless opportunities for workflow and systems to be more efficient and easily controlled. Everything from window shades, to light switches, to televisions and thermostats can exist in harmony with conventional building systems, information technology systems, and clinical systems on one unified network.

However, while designing your hospital to achieve this level of connectivity has a many benefits, it also opens you up to greater vulnerabilities. Each device that is connected to your network represents a potential intrusion point from a cyber security perspective. Often, since these less-technical devices wouldn't fall under their purview, your IT department may not even be aware of certain access points to your network.

So, how can hospitals protect their complete cyber infrastructure — from computers to window shades — from malicious attack?

A Holistic Approach to Cyber Security

The answer involves taking a holistic approach to cyber security. This requires a level of sophistication to recognize that creating a secure cyber infrastructure involves more than protecting the computers and tablets in your hospital. It starts with the approach to planning of the hospital. Because of the Internet of Buildings, planning of information technology, building systems, and clinical equipment can no longer be carried out in silos. There must be a single, unified process that considers those systems holistically.

As the connectivity of devices and objects in their building grows, many hospitals also are utilizing cloud-based storage. Shifting the storage and processing of sensitive medical data to a third-party cloud provider allows hospitals to outsource portions of their network security as well. By storing electronic medical records and hospital servers in a cloud environment, this data is protected by the cloud provider's world-class experts in cyber-security – perhaps a level of expertise that few hospital systems can match. In addition, any intrusion that could come through a device on the Internet of Buildings at the local level would be impeded from accessing important patient data because of improved network segmentation.

However, this solution won't be the right fit for every hospital and the decision to have portions of your network be cloud-based or on-premise involves multiple considerations.

Summary: With so many systems with network connections — from audio/video systems, to security systems, to clinical equipment — your hospital may have hundreds of different types of devices that utilize some type of connectivity. Recognizing this vulnerability and expanding your concept of cyber security to holistically include all of these potential threats is the first step in creating a more resilient hospital cyber infrastructure.

Conclusion

While “healthcare resiliency” may seem like nothing more than a catch phrase, the purpose of this broad goal is simple: to allow facilities to care for their patient population, regardless of circumstances. And when patient safety and hospital functionality is at stake, there’s no room for cutting corners.

With each of these five key areas of healthcare resiliency, hospitals would be well served to consult with experts and outside perspectives. However, when you’re undergoing a facility or vulnerability assessment, look for consultants and engineers with a dedicated healthcare focus. The healthcare industry is unlike any other in its demands, and a healthcare-related specialist versed in MEP infrastructure, physical security, or cyber security can better provide your hospital with the exact resources and insights you need to move forward, implementing mitigation actions to remedy vulnerabilities.

True healthcare resiliency, however, doesn’t stop there. It should be an ongoing process that is continually assessed and reviewed, alongside a consistent education and training program for hospital staff.

It’s an unfortunate truth of life: you can’t prepare for every harmful scenario that comes your way. However, with the proper insights and expertise, you can create a hospital that is prepared to be resilient in the face of challenges.