COSMOS
Navigate the Compliance Universe

Compliance Today - January 2023

François Bodhuin (bodhuinf@ihn.org, linkedin.com/in/francois-bodhuin-a8556916/) is Assistant Vice President and Chief Information Security Officer at Inspira Health, Vineland, NJ.

Gerry Blass (gerry@complyassistant.com, linkedin.com/in/blass-917a482/) is CEO at ComplyAssistant, Colts Neck, NJ.

Hope for the best, expect the worst, plan today

By François Bodhuin and Gerry Blass

The evolution of the risk of successful cyberattacks has been evident since 2010—when the Affordable Care Act was signed and resulted in a transition from paper to electronic medical records. Healthcare organizations began implementing new electronic medical record applications to comply with meaningful use (MU) requirements. Over the years, MU has introduced new criteria with a heavy focus on interoperability among applications. The combination of MU efforts, merger and acquisition activity, and the pandemic-induced remote workforce have increased healthcare organizations' risk profiles, remaining a prime target for cyberattackers to do what they do best.

There are numerous reasons for the high level of cybersecurity risk in healthcare, such as limited staffing and the technology required to effectively implement controls that reduce risk. These scenarios contribute to higher risk at almost every level of the organization. As a result, we have witnessed successful cyberattacks that have resulted in healthcare organizations experiencing extended downtime for a critical application, their entire network, or somewhere in between.

Furthermore, only 54% of businesses have a documented, community-wide disaster recovery and business continuity (DRBC) plan.[1] Unfortunately, some business executives have taken the "it won't happen to me" approach, and the results can be devastating.

This article is based on more than 60 years of experience in the industry to arm your team with five key questions to consider when implementing a DRBC plan. Now is the time to prepare for the worst.

Question 1: Why do I need a DRBC plan?

The first step in developing a DRBC plan is understanding its purpose. Disaster recovery defines how an organization's IT department will recover from a natural or manufactured disaster, such as restoring necessary applications. Business continuity focuses on the business operations side of DRBC, such as downtime procedures for vital departments and applications.

In today's environment, it is essential for the enterprise emergency management team to understand that cybersafety has a direct line to patient safety. An extensive, successful cyberattack can bring down medical devices and divert patients to other facilities for necessary treatments such as chemotherapy, dialysis, and

intensive care unit (ICU) services. In the past, we would see downtime generally lasting up to 72 hours, whereas today, that number has increased to a month or more. This disruption devastates the healthcare system and the patients who depend on critical care.

It is important to ensure the DRBC plan aligns with an organization's emergency management plan, incident response plan, business impact analysis (BIA), and extended departmental downtime/business continuity procedures.