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.

Question 2: What does extended downtime mean for my business?

We know the systems and technology used at the healthcare-organization level require maintenance. When this occurs, downtime is planned, and procedures are implemented to safeguard advanced notice to staff and minimal disruption to patient care. Unfortunately, what we’ve seen more often in the past couple of years is incident after incident of “unplanned downtime.” Whether it’s the result of ransomware or a natural disaster, these situations can be costly and sometimes deadly.

An IBM survey published in July 2021 found that healthcare breaches cost the most of any industry, averaging $9.23 million per incident, which is $2 million more than in 2020.[2] These numbers continue to grow, putting hospitals in a significantly worse place than they’ve been in years. The bottom line? Whether your system is down for three days or three months, there are detrimental consequences with every passing day. Having a plan won’t certify that bad things won’t happen, but it *will* confirm that your organization is better equipped to handle them.

Question 3: What does third-party risk have to do with DRBC?

According to the Federal Deposit Insurance Corporation, various types of third-party risk can impact an organization on numerous levels.[3] These include compliance, reputation, strategic, operational, transaction, credit, and country risks. At Inspira Health, a leading charitable nonprofit healthcare organization in southern New Jersey, along with other systems around the country, the chief goal of the chief information security officer (CISO) is to guarantee patient data and lives are protected. While it takes seconds for a patient’s protected health information (PHI) and safety to be compromised, it can take weeks or longer to resolve the issue.

Having a DRBC plan in place can help reduce third-party risk and prepare for extended downtime. It is imperative that organizations, regardless of size, assess potential risks as low, medium, or high and plan accordingly. Vendors without access to PHI tend to rank on the low-risk side, and vendors with PHI access are typically in the medium to high-risk category. The average hospital has relationships with vendors of varying risk levels, so conducting periodic BIAs can help establish and maintain the efficacy of your DRBC plan.

Third-party vendors that rank as high risk for your organization must demonstrate that they are working proactively to remedy the underlying issue(s). The process from here is dependent upon both parties. As the entity, you must ensure you’re not bringing excess or unnecessary risk into the organization, and the third party must take action to address any potential risk. If these actions can’t be achieved in a suitable time frame, it is up to the organization to consider further action.

Question 4: How can I collaborate with other departments in my organization on DRBC?

After you’ve assessed your major third-party vendors and applications and taken steps to remedy any high-risk threats, the next step is to bring together the proper stakeholders. This team should include leaders from each pertinent department, such as:

- Legal
- Risk management
- Compliance
- IT/security
- Nursing
- Ancillary departments (radiology, laboratory, pharmacy, etc.)
- ICU, emergency department, learning and development
- Finance/human resources/public relations/accounts payable
- Facilities

A tight-knit team helps verify that nothing falls through the cracks, and each stakeholder can account for their respective department's needs. For example, how long can the finance team keep paying employees if the payroll system is down for an extended time? How does an extensive period of enterprise downtime impact billing, patient care, and interdepartmental communications? These, and more, are considerations in DRBC planning, so it's vital to keep everyone involved throughout the process. Ongoing collaboration and communication will support the overall workflow and necessary procedures to the organization and confirm the continuum of patient care.

An enterprise-wide team will help guarantee that crucial considerations aren't missed or discounted when developing and implementing your plan. It's always enlightening to bring groups together and find that various departments offer vastly different ways to handle a particular issue. While the responsibilities of the team members will vary, some of the valuable roles and tasks include:

- Working collectively to create a BIA
- Assessing the impact of each department's low, medium, and high-risk levels
- Ensuring that high-risk vendors are closely monitored and BA agreements outlining liability are thoroughly assessed
- Identifying the maximum amount of time each department can maintain operations if disaster strikes
- Attending team meetings consistently to check on progress

Question 5: What advice would you give CISOs, information security officers, and other health information managers/professionals?

Start today. Don't delay your efforts to bolster your organization's DRBC plan. While the landscape has changed drastically over the years, one element that hasn't shifted is the reward of being proactive regarding cybersecurity. Though DRBC plans vary across organizations, the essential element is that each organization has a plan so that if a disaster occurs, leaders are prepared to make timely, effective decisions.

The following are some tips we've learned over the years that have contributed to our success.

- **Reduce the risk of a successful cybersecurity attack.** In the fall of 2019, the Office of the National

Coordinator for Health Information Technology assigned the U.S. Department of Health & Human Services 405(d) Taskforce to establish the Health Industry Cybersecurity Practices (HICP) in partnership with the National Institute of Standards and Technology and Office for Civil Rights.[4] Collectively, the team identified the five main threats in cybersecurity:

  - Email phishing
  - Ransomware
  - Attacks against connected medical devices
  - Insider, accidental, or intentional data loss
  - Loss or theft of equipment data

Additionally, the team identified 10 controls, or ways to mitigate, the most common threats. HICP and DRBC should go hand in hand because they allow organizations to determine which risks are most relevant and the best ways to alleviate them.

- **Conduct ongoing BIAs.** Invest the time to thoroughly assess your key departments, applications, *and vendors*. It is fundamental to keep your BIA current to account for change management. This activity impacts your DRBC plan and procedures as well as the related plans previously listed. Since a large percentage of successful cyberattacks have originated at the vendor location, implementing a comprehensive, third-party risk management program is crucial. Whether you have one significant application from a vendor, or multiple critical applications (e.g., medical devices vendor), it is important to vet them when they are onboarded and periodically thereafter.
- **Consistency is the DNA of success.** Your DRBC plan and related plans should undergo tabletop testing exercises on a reasonable frequency based on several factors, including organizational size and scope, results of previous tests, and change management (e.g., organizational change and modifications to your network, applications, etc.).
- **Outsource, outsource, outsource.** When there are challenges with internal resources and a need for outside, unbiased subject matter expertise, consider engaging a virtual CISO organization to help fill gaps and provide another set of eyes and ears. The scope of the current risk terrain is significant, which makes outsourcing a potential strategy to enhance your internal resources to reduce the risk of a PHI breach and protect your patients' safety and lives.

Takeaways

- Understand the current landscape as it pertains to cybersecurity, which includes challenges brought on by the remote workforce and impending threat of extended downtime.
- Know the value of a disaster recovery and business continuity plan, including alignment with an organization's emergency management plan.
- Recognize the various types of third-party risk outlined by the Federal Deposit Insurance Corporation, including compliance, reputation, strategic, operational, transaction, credit, and country risks.
- Discover how to build a high-impact team within your organization, which should include stakeholders from legal, risk management, compliance, IT, nursing, and ancillary departments.

- Learn from your peers. Do not hesitate to copy a methodology if it has been successful and makes sense in your environment.

---

1 GFiuui45fg, "Only 54% of organizations have a company-wide disaster recovery plan in place,"*Cyber Reports*, June 29, 2021, https://cyber-reports.com/2021/06/29/only-54-of-organizations-have-a-company-wide-disaster-recovery-plan-in-place/.
2 "IBM Report: Cost of a Data Breach Hits Record High During Pandemic," *IBM*, July 28, 2021, https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic.
3 "VII. Unfair and Deceptive Practices—Third Party Risk," *FDICConsumer Compliance Examination Manual*, June 2019, https://www.fdic.gov/resources/supervision-and-examinations/consumer-compliance-examination-manual/documents/7/vii-4-1.pdf.
4 National Institute of Standards and Technology, Office for Civil Rights, *405(d) Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)*, 2019 https://www.nist.gov/system/files/documents/2019/10/16/1-4-hicp-405d-chua-decker-heesters.pdf.