Industry: Healthcare
Services: IT services, managed IT services, IT support services
Solutions: Data protection, disaster response & recovery

How Prompt Discovery & Action Secured Multibillion-Dollar Business Continuity During Cyberattack

Climate (282 words)

Expanding Risk Landscape

In the past year, the cyber threat landscape has changed significantly for businesses. With the advantages of digital business transformation also comes a dark underbelly of *unprecedented cyber risk*, pressing CIOs to take another look at the viability of their cybersecurity strategies. As recent as 2018, IT services' boardroom focus was mostly directed at achieving compliance whereas, today, the *rapid acceleration in technology trends* is introducing more risk than ever. **Healthcare companies are a natural target**, given the volume of highly sensitive data handled routinely. Most recently, the *rise in remote work* has added another point of vulnerability to the plethora of potential threats that now cost healthcare companies an astounding average of USD 9.42 million—*per incident*.

Collective Belief that Cyberattacks are Infrequent or Overstated

Similar to how school-age students practice what to do in a tornado or fire drill but can't really know what to expect in real life, internal **IT teams often consider cyberattacks to be anomalies** that can't really be prepared for. The unfortunate result is that, in the midst of an actual threat, *often practical, thorough, up-to-date response plans are absent* and what is available is inadequate.

Personnel tasked with managing day-to-day IT operations rarely make sufficient time for the critical maintenance that impacts overall IT health and security. The role can sometimes even morph into an IT support services concentration on time-consuming help desk support, provided to internal customers.

When Technology Isn't Working, Customer and Business Needs Aren't Being Met

In this case study, we look at how managed IT services provider, *Path Forward IT*, helped one multibillion-dollar healthcare business *quickly contain a malware attack*, *ensuring continuity of vital services* for its customers.

Background (118 words)

The Incident

The subject of this study is an oncology products and services provider with global reach. A security breach to its first-generation, cloud-based storage system impacted only U.S. locations—including 1,215 customers and thousands of cancer patients.

To contain the threat and ensure patient privacy was protected, radiation equipment was taken offline until the issues were resolved. The oncology software is used on linear accelerators for radiation treatments. Systems were offline for more than a week before external assistance was sought. In the near term, some cancer patients were transferred to other healthcare providers to continue their treatments. Around 170 customers that use the first-generation cloud system, experienced service disruptions to one or more of their products.

Challenges (310 words)

Lack of Visibility

Though there was an IT vendor in place for the client, they were scrambling to isolate the problem. There was no visibility into the infrastructure, and information and data provided was incorrect. Patients were irritated that, when they arrived for treatments, the vendor simply told them, "We don't have your data and aren't seeing patients."

The client was scrambling to gather customer lists and data. The service sites—known as patient centers—were small, and some didn't have an IT team. *PathForward IT* was able to step in, on the fly, to figure it out once engineers were onsite.

> *"We (PathForward IT) typically take a preventative approach, working with clients to plan for these types of disruptions and would have known what equipment was at each site but, because this was a new customer, we didn't have all the data needed at the time of the event."—Adam Brock, Senior Director, Data Protection, PathForward IT*

Recovery Time Critical

When it comes to criticality of recovery time, systems impacting cancer treatments would obviously rank as a serious, high priority. Because some terminally ill patients were experiencing treatment delays, restoring and getting operations back online immediately was of utmost importance. But that isn't necessarily as easy as it sounds… especially in this unique scenario.

In a cloud breach, this client needed hardware and people resources onsite; custom hardware built to meet their specifications and configured to work; and a trained engineer to install and operate the hardware and work with third parties to finish the software configuration.

Unexpected Pandemic

As though the complexity of conducting an urgent IT response effort, in a critical health segment, wasn't challenging enough under "normal" circumstances, in this case, logistics and the ability to acquire hardware and parts were both extra challenging due to a global Covid-19 pandemic. Travel was restricted during this time and engineers were located in different time zones. If a project lead could get a flight, there was a probability of extended layovers. Sourcing materials was difficult because parts and hardware just weren't available. U.S. package delivery services were also in a state of confusion and unreliable at this time, adding to the mix of obstacles.

Solutions (521 words)

Prompt Discovery, Organization & Action

PathForward IT began engagement with the client by kicking off a discovery call to determine needs and expectations. The issues investigation and troubleshooting were performed remotely from the home office, freeing up on-call engineers to answer questions across all client sites.

The general solution base (small, medium, large) was determined first, then refined by each location's specific needs. From there, an inventory of the various patient centers was created, defining the equipment type(s), power status, and ship to information of each location.

"Due to strong in-house expertise, much of the issues investigation and troubleshooting was able to be performed remotely, freeing up engineers to be on call to answers questions across all client sites."—Tessa Anderson, Director, Project Management, PathForward IT

Once the inventory was complete, equipment quotes were sought, approved by the client, and sent out immediately from a *PathForward IT* trusted vendor.

Engineers traveled to 11 different sites within the U.S.—some to multiple sites—to deploy, configure and install hardware and software. Project engineers assisted remotely, ensuring the work could be done quickly and efficiently.

With the collective team effort, customer data was promptly secured, and the client was back to seeing patients within a week. Some patient centers were ready to go back to the cloud as hardware orders and site revisits continued.

> *"One of the advantages of bringing in our team of experts was the ability to rapidly scale the entire recovery operation—from on-call engineers conducting remote troubleshooting, to dedicated leads on-prem at each of the client's impacted cancer sites."—Mindy Smyth, Vice President of Communications, PathForward IT*

Deep Expertise in Specialized Area

With cancer patient centers in different parts of the country, each location had nuances. But, to address problems as quickly as possible, it was crucial for project engineers to initiate much of the work before the engineers were even onsite. From a technical standpoint, healthcare is one of the most complicated industries. To assist remotely in this type of scenario required subject matters with deep understanding of healthcare environments, priorities and protocols; experience with multiple records systems; and a working knowledge of HIPAA compliance, rules and regulations.

PathForward IT was already very familiar with the equipment needed for oncology centers, from the subtleties—such as, a printer going down meant inability to label vials—to how highly specialized oncology is—like how drug cabinets have to be networked. Because of the nuances, most solutions needed to be very customized for each customer location.

Even with the specialized, custom solutions, by virtue of having served healthcare practices for 20+ years, *PathForward IT's* responsive business model enabled them to get hardware shipped and installed at every site faster than the time it took the IT vendor to get it up and running.

Values & Relationships

***PathForward IT* takes their core values of service, ownership, respect, transparency, integrity and empathy seriously and it shows in the way they conduct business. Knowing the criticality of cancer patients receiving their treatments in a timely and consistent manner, they embraced their "service-first" culture and didn't let obstacles stand in their way.**

- Adaptability - when the staff couldn't get flights, one team member connected with a friend of a friend who was already in the client's area and sought their help in sourcing materials.
- Scalability – highly-skilled, valuable resources were able to be scaled to manage, implement, and support the recovery effort, from end to end, until services were up and running.
- Preparedness - through the longstanding relationship that *PathForward IT* has with the client, they were able to quickly jump in, scope, and get teams onsite to assist and minimize the impact to patient care.

Path Forward IT

At *Path Forward IT*, our mission is to improve our clients' efficiency and effectiveness with unbiased guidance, seamless IT systems and applications support, and an unrelenting commitment to service. We dedicate the time to truly listen to every client's business objective, evaluating where they stand today and providing unbiased insight on which services and solutions will truly meet their objectives. Every client we work with receives our undivided attention as we work together to create more efficient and resilient businesses.

Relevant Stats (for imagery / infographic)

- Average cost of a healthcare data breach is USD 9.42 million
- Multibillion-dollar healthcare company
- PFIT team of 13
- Hardware delivered, configured and deployed to 11 different US locations
- 1,215 US-based client customers impacted
- 240 total hours spent securing patient sites
- Recovery implemented within 5 days
- 98.5% PFIT client satisfaction

For More Information

https://www.pathforwardit.com/industries/healthcare/ and https://www.pathforwardit.com/solutions/data-protection/