



Mary Rutan Hospital



Table of Contents

- Overview 3
- Cybersecurity Trends. 5
- Solutions 10
- Next Steps 12

Overview

In an age of escalating cyber threats, the healthcare sector remains a prime target for malicious actors. Hospitals, with their vast stores of sensitive patient data, are particularly vulnerable.

Demonstrating exceptional IT leadership, Mary Rutan Hospital has taken a proactive stance by developing a robust and comprehensive cybersecurity strategy.

Fortifying the hospital's defenses against phishing and malware attacks, the organization emphasizes the crucial role of employee awareness and training. By focusing on educating staff about the latest cyber threats and best practices, Mary Rutan Hospital sets a benchmark in safeguarding patient information and ensuring the integrity of its healthcare services.





About Mary Rutan

In operation since 1919, Mary Rutan is a general medical-surgical hospital dedicated to providing high-quality patient care. Located in Bellefontaine, Ohio, Mary Rutan Hospital serves the healthcare needs of the local region. Multiple expansions have occurred during the organization's 100-plus-year history and each time the organization increased services offered to the community.

"We are a typical rural healthcare organization," said Mary Rutan Hospital IT Director and HIPAA Security Officer, Robert Reynolds. "This includes a full-service hospital with surgery suites, family care offices throughout the region, and different specialty clinics. We try to do as much as we can for the area."

Inspired by this dedication to care, the organization has prioritized the safety and privacy of patients, employees, and stakeholders with achievement goals in cybersecurity.



500+
EMPLOYEES



\$100M+
ANNUAL REVENUE



100+
YEARS OF PATIENT CARE

Cybersecurity Trends

While the ongoing digitization of healthcare has promised to enhance the patient experience, improve efficiency, and drive innovation, these promises come with a host of challenges, particularly for the teams managing the technological integration within healthcare organizations. In an industry that prioritizes privacy, for example, cyberattacks have emerged as a key concern.

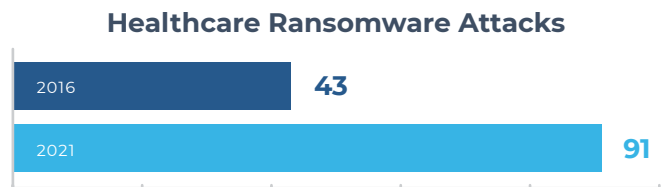
1. Higher Risks and Costs Associated with Attacks

Large-scale healthcare cyber incidents like that of the [2015 Anthem medical records breach](#) and subsequent \$16 million 2020 HIPAA settlement, as well as the recent 2024 [Change Healthcare](#) ransomware attack, have brought the issue of security to the forefront.

As a result, business leaders increasingly recognize the need and value of a strong cybersecurity posture.

“With the recent Change Healthcare attack, you see a multi-billion dollar a year company that is vulnerable,” said Reynolds. “It’s a wake-up call.”

Statistically, these types of targeted attacks are on the rise as noted in the [JAMA](#) healthcare study that found the annual number of ransomware attacks on health care delivery organizations more than doubled from 2016 to 2021, exposing the personal health information of nearly 42 million patients in the process.



With the widespread reporting surrounding the dangers of a cyber event, organizational awareness of the level of risk involved has fortunately also risen.

DID YOU KNOW?



91%

of all cyberattacks begin with a phishing email



1 in 3

successful breaches involve the use of phishing techniques



Over half

of ransomware attacks originated with a phishing email

SOURCE: Deloitte & University of Maryland

Managing Change While Staying Compliant

2. More Organizational Awareness

When it comes to cyber risks, organizational leaders and other stakeholders in the healthcare field are increasingly aware of the potential consequences.

“Cybersecurity is becoming more top of mind for everybody,” said Reynolds. “In that way, selling the need for strong cybersecurity has become easier to do and easier to justify.”

Developing adequate cybersecurity strategies requires an understanding of how a breach can occur. One of the ways that criminals get into business systems is through phishing attempts.

According to the National Institute of Standards and Technology (NIST), a phishing attempt is a technique for attempting to acquire sensitive data through a fraudulent solicitation in an email or on a website, in which the perpetrator masquerades as a legitimate business or a reputable person.



As a result, it was important to Reynolds and his team to establish a method by which to keep employees and other stakeholders informed and to build on their existing cyber awareness to prioritize safety for all.

No amount of money that we spend on cybersecurity matters if a member of our staff clicks the wrong link and a cyber criminal gets through. BlueOrange has helped us formulate that message and we promote it throughout our organization. That’s been really positive.



Robert Reynolds

Mary Rutan Hospital IT Director and HIPAA Security Officer



3. Cybersecurity Prioritized

With this new level of awareness, cybersecurity can be more easily prioritized to individuals outside of the information technology teams and generalized to everyone with access to business systems.

“It has been in the last two to three years that changes really started to take place and the big shift has been financial,” said Reynolds. “It wasn’t so much that the organization was not aware or able to acknowledge that these cybersecurity risks were there. It was more an issue that some of the solutions are fairly significant investments. If you’re deploying a full cybersecurity suite, that’s 24/7 monitoring of your network. It can be a big investment for an organization.”

Within this paradigm shift, businesses are more universally considering cybersecurity protection as an essential, rather than a nice-to-have, or an insurance product.

“Smaller healthcare organizations have limited funds and will invest the majority of their dollars to enhance patient care,” said Reynolds. “Major investments in cybersecurity have historically been viewed as luxuries or insurance products. The thought before was that in case something

happens, then we will have that protection. But now, it isn’t if something were to happen, it’s when it does, so you need to build your capabilities around that logic.”

Considering the inevitability of an attempted breach, Reynolds and his team sought to put in place a series of protective measures that would position the organization as an unattractive target for would-be hackers.



Annual Number of Ransomware Attacks on Healthcare

2X Increase

FROM 2016 TO 2021

42 Million

PATIENT RECORDS EXPOSED

>44%

INCIDENTS DISRUPTED THE DELIVERY OF CARE

SOURCE: JAMA

4. Adopting a Proactive Security Posture

Increasingly, organizations are taking a more proactive posture with cybersecurity and compliance which is saving money, not only in the avoidance of costly penalties, but also in the case of insurance premiums.

When it comes to cybersecurity, Reynolds stresses the importance of also staying one step ahead of the pack.

“I use an analogy when it comes to cybersecurity,” he said. “It’s like being chased by a bear. You don’t have to be faster than the bear, you just don’t want to be the slowest person in your group. Cybersecurity is the same way. You don’t have to be the best, but your system must be difficult and protected enough that bad actors want to move on and not mess with you. We’re trying to have a reasonable goal of being difficult enough that they move on to easier targets.”

To do so, Reynolds recommends a multi-faceted approach that employs various strategies to prevent unauthorized access.

“I think the mindset has changed from being a reactive type of solution to utilizing more proactive products. You want to be able to say that you are preventing things from happening and shutting things down before they happen, but there are also cybersecurity insurance rates and deductibles based upon the controls that you put into place.”



An Assessment of Risk



“The effort to educate staff has been perhaps one of the biggest benefits of BlueOrange.”

5. Multifaceted & Holistic Security Strategies

In addition to deploying software solutions, the team at Mary Rutan Hospital ensures that processes contribute to a robust security environment.

“It’s a lot about training and educating staff,” said Reynolds. “We want to achieve that balance of having all the right protections in place but if you’re ignoring staff education, you may as well not spend anything, quite frankly.”

With an awareness of the many trends driving change in an already dynamic industry, Reynolds and his team partnered with BlueOrange Compliance to ensure that their cybersecurity and compliance posture would position them for success.

5 HEALTHCARE CYBERSECURITY TRENDS

Reynolds and his team have identified five trends that have emerged for cybersecurity professionals in healthcare which are:

①

Larger risks and costs associated with attacks

②

More organizational awareness to the potential consequences of a cyber incident

③

Cybersecurity is prioritized as an essential element of a successful overall business strategy

④

Organizations are increasingly adopting a proactive security posture

⑤

Successful security strategies that are multifaceted and holistic in approach

Solutions

BlueOrange Compliance has helped Mary Rutan to fulfill key goals in the area of cybersecurity preparedness and compliance.

“We have been able to knock down some of the big blocks and get to a better position for continual improvement.”

Having a partner like BlueOrange Compliance can help to provide organizations with guidance they need to see it through.

“It was BlueOrange Compliance that really helped us to get a plan developed for how to chip away at it because it is the elephant in the room,” said Reynolds. “There’s no way you can just uplift a cybersecurity program to any organization. You have to build it in phases just to bring the cybersecurity program up to speed.”



BlueOrange guided the hospital in prioritizing cybersecurity efforts each year.

“It’s been incremental over the past four years,” said Reynolds. “We’ve been working with BlueOrange and we have seen steady improvement. BlueOrange helped guide us and let us know where the specific priority should be each year and kept us going.”

“BlueOrange helped guide us and let us know where the specific priority should be each year and kept us going.”

Additionally, BlueOrange has helped Mary Rutan Hospital to communicate the value of cybersecurity and compliance to hospital leadership, building a strategy that is proactive.

“BlueOrange also helped in the sale of the need for cybersecurity to the administration,” said Reynolds. “BlueOrange was able to have the backing, the expertise, and the information that we can share with leadership that shows what these programs do and what it means. It isn’t just an individual employee screaming that the sky is falling. It’s a respected organization that has shown cybersecurity doesn’t have to be overly cumbersome or intrusive to the user or the organization. It’s something that we can build into the workflow and make it as commonplace as it can be for users so that they’re not rejecting it and they are accepting.”



Going Forward

“With BlueOrange, we have been able to knock down some of the big blocks and get to a better position for continual improvement.”

In addition to their guidance and expertise, Reynolds and his team have appreciated the way BlueOrange has kept the organization informed of ongoing trends, security incidents, vulnerabilities, and other key cybersecurity issues in real time through the BlueOrange Compliance Security Alert System.

The security alerts are sent automatically to BlueOrange customers when a new potential threat is detected. It is a system created to keep businesses aware of new cybersecurity threats.

“The effort to educate staff has been perhaps one of the biggest benefits of BlueOrange,” said Reynolds. “When we receive one of the security alerts, we send them to the staff to help boost employee education. Particularly when it comes to phishing and malware because no amount of money that we spend on cybersecurity matters if a member of our staff clicks the wrong link and a cyber criminal gets through. That’s the kind of message that we keep repeating. BlueOrange has helped us formulate that message, and we promote it throughout our organization. That’s been really positive.”

Next Steps for Cybersecurity

The most effective way to combat these types of attacks is through education of the workforce. With BlueOrange Compliance Alerts, Reynolds and the rest of his team at Mary Rutan are able to keep employees and other stakeholders informed, giving everyone a personal stake in online safety, both at work and in their everyday lives.

“The security alerts let us know if a malware variant or specific attack vector is propagating and increasing. Once we have the information, we will send out a warning to everybody. It has been very well received. Not only is it in the employee’s best interest to keep Mary Rutan Hospital safe, but they need to learn these things to keep themselves safe at home. We make it personal to them and keep it top of mind every day for their online banking, credit card use online, anything. It’s important to pay attention to protect yourself, and it resonates for everyone.”



To learn more about BlueOrange solutions for cybersecurity and compliance, **visit our website today.**

[Learn more →](#)

Inspired by Mary Rutan's success story?

Connect with us to begin your own cybersecurity and compliance journey.



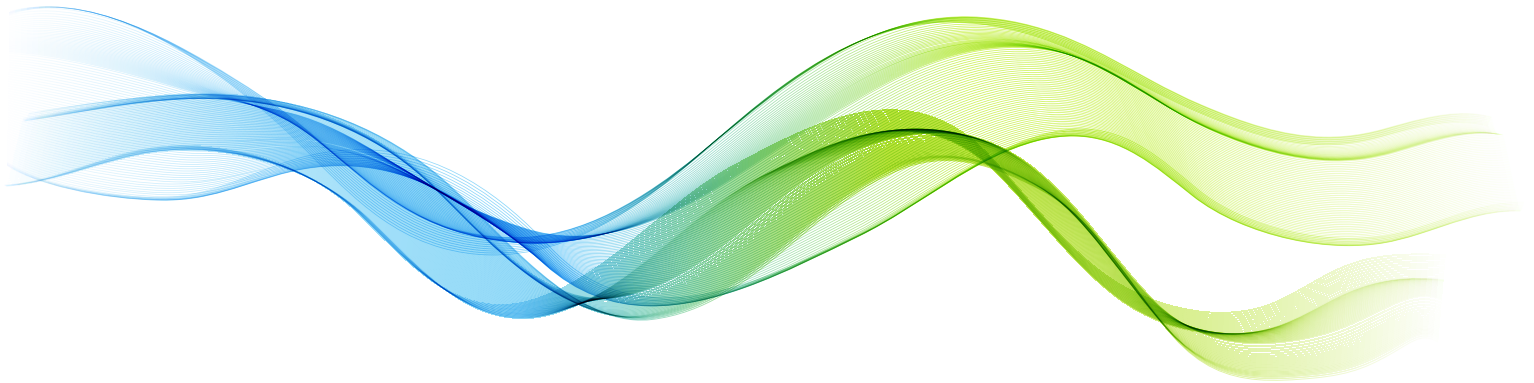
855-500-6272

BlueOrangeCompliance.com



877-991-1991

GoCloudWave.com



ABOUT BLUEORANGE COMPLIANCE

BlueOrange Compliance, a CloudWave company, is a leader in information privacy and security, regulatory compliance, and risk management services. Together with CloudWave, BlueOrange Compliance delivers end-to-end cybersecurity solutions for healthcare organizations facing increasingly complex compliance landscapes, including HIPAA, HITECH, OCR, and other industry-specific regulations.

The combination of our proven track record in compliance audits, risk assessments, cybersecurity testing and training, and cybersecurity consulting and risk management services along with CloudWave's advanced threat detection, incident response, and cloud infrastructure capabilities results in a comprehensive set of offerings that empower healthcare organizations to secure sensitive data, streamline compliance efforts, and mitigate evolving cyber threats.

ABOUT CLOUDWAVE

CloudWave is a full-service cybersecurity and cloud services provider built exclusively for healthcare. Protecting over 350 hospitals and health system environments, CloudWave delivers end-to-end solutions that combine secure hosting, IT operations, and 24/7 threat detection and response. Services include managed security, risk and compliance, disaster recovery, systems management, and cloud optimization—all delivered with a healthcare-first mindset. Powered by AI-driven security operations and supported by U.S.-based Network and Cybersecurity Tactical Operations Centers, CloudWave provides a cyber-ready foundation for safe, uninterrupted patient care.