WHEN CYBERATTACKS HIT, DISASTER RECOVERY IS NOT ENOUGH

HEALTHCARE IT PROFESSIONALS WEIGH IN ON NEW WORLD CYBER SECURITY AND RESILIENCE REQUIREMENTS

AUTHORED BY:

BECKER'S
HEALTHCARE

UNDERWRITTEN BY:

IRON MOUNTAIN®

WHEN CYBERATTACKS HIT, DISASTER RECOVERY IS NOT ENOUGH

HEALTHCARE IT PROFESSIONALS WEIGH IN ON NEW WORLD CYBER SECURITY AND RESILIENCE REQUIREMENTS

In healthcare, the stakes could not be higher when it comes to cybersecurity. Organizations need to prevent the potential loss of revenue and erosion in brand reputation and patient trust. A healthcare breach increases patient churn by 6.7 percent and results in a reputational loss worth nearly $4 million, not counting the estimated $1 million necessary for breach remediation, according to the Institute for Critical Infrastructure Technology.

Unfortunately, the rate of successful cyberattacks is proving there is no such thing as 100% prevention. A recent study by IDG and Iron Mountain revealed that, despite the heavy focus on prevention, nearly 40% of healthcare organizations have experienced a ransomware attack.

Leveraging insights gathered through roundtable discussion with nine hospital and health system IT leaders, this Healthcare ebook will explore new world cyber security and resilience requirements and provide an up-to-date perspective on the:

- Emerging challenges contributing to the complexity of managing data protection and cyber resilience.
- Implications of the healthcare industry’s heavy focus on prevention.
- Strengths and deficiencies of traditional backup and recovery methods.
- Critical considerations for delivering a balanced cyber resilience plan.

> “In 2016, the Institute for Critical Infrastructure Technology declared healthcare as the most targeted yet underprepared sector within the United States’ critical infrastructures.”

CHALLENGES CONTRIBUTING TO THE COMPLEXITY OF MANAGING DATA PROTECTION AND CYBER RESILIENCE

Today's cybersecurity threats are intense enough to render hospitals' traditional security playbooks nearly obsolete. The protection strategies most healthcare organizations have in place are not designed to sufficiently protect and restore critical data with the assured integrity and expediency required to resume normal patient care and business operations quickly after an attack.

Several factors contribute to this reality.

1st: The cyberthreats hospitals face are growing more sophisticated and exceeding the abilities of historically tried and true prevention strategies. Effective cyber resilience strategies contain four pillars: prevention, protection, testing and recovery. Yet, sixty-one percent of healthcare organizations say the cybersecurity measures they have in place largely focus on prevention.

2nd: As the types of cyberthreats continue to expand, the healthcare industry remains a primary target due to the vast amount of digitized data available. In 2016, the Institute for Critical Infrastructure Technology declared healthcare as the most targeted yet underprepared sector within the United States' critical infrastructures.

3rd: Healthcare organizations are not scaling their cybersecurity defenses to account for scenarios across the board – from initial threat to recovery from a successful attack. Prevention efforts are important but so are recovery capabilities, which the majority of healthcare organizations do not feel confident in. Sixty-nine percent of healthcare organizations believe their data protection infrastructure is inadequate to recover from cyberattacks.

4th: Although hackers and attacks are growing more sophisticated, health IT professionals and executives have not seen meaningful gains to their security budgets. In spring 2018, Black Book Research surveyed more than 2,400 security professionals from 680 provider organizations. Eighty-eight percent said their IT security budgets remained level since 2016.

Taking this into account, it's become critical for CISOs to explore a cyber resilience strategy that balances resources across all National Institute of Standards and Technology framework requirements to address the protection and recovery of critical data if – or really when – an attack occurs.

HEAVY FOCUS ON PREVENTION RESULTS IN UNBALANCED CYBER RESILIENCE STRATEGY

Cybersecurity threats today demand layered defenses. Health systems that continue to put the majority of their resources into prevention are not immune from cyberattackers, who are only growing more sophisticated. "I mean, they're able to begin to get around our firewalls, mimic habits of personnel," the chief technology officer with a 48-bed community hospital in the Midwest said during the Becker's-Iron Mountain roundtable. "I also believe the cost of prevention, or trying to keep up with prevention, is a big challenge, as is the personnel to manage it – especially for smaller institutions."

Hospitals and health systems that underinvest in the protection, testing and recovery aspects of a cyber resiliency strategy are taking a gamble. When an attack occurs – overthrowing any prevention investments – these enterprises are poorly positioned to recover data whose integrity has been tested and validated in a timely manner. As a result, excessive downtime often ensues, putting their reputation, quality of patient care and revenue at risk.

The CTO with the 48-bed hospital in the Midwest said he sees reputational costs, lost revenue from downtime and business continuation expenses as the greatest risks of poor resiliency capabilities. "To be down for even one day, for any of our institutions – and we're a small institution – is a pretty big impact," he said. "And in a small community, reputation matters."
In addition to reputational costs, weak post-attack recovery capabilities can leave already troubled hospitals incurring massive operating costs, losing revenue via canceled procedures and diverted care until they're back up and running.

"Just a simple phishing attack can waste thousands of IT hours and alone dramatically impact operations," said the CTO of a 484-bed academic medical center and Level I trauma center in the Midwest.

"It can be a huge disruption to the organization, which is going to of course have downstream financial and reputation cost."

Especially troubling is the possibility of healthcare organizations falling into a sense of false security, where

BY THE NUMBERS:

THE STATE OF HEALTHCARE CYBER SECURITY

- A healthcare breach increases patient churn by 6.7% and results in a reputational loss worth nearly $4 million.

- Nearly 40% of healthcare organizations have experienced a ransomware attack.

- Sixty-nine percent of healthcare organizations believe their data protection infrastructure is inadequate to recover from cyberattacks.

- Eighty-eight percent said their IT security budgets remained level since 2016.

prevention investments avert leaders' attention from post-attack processes and abilities. Many organizations have never conducted live testing of their business continuity or disaster recovery plans. The survey Black Book Research conducted in spring 2018 found 83 percent of healthcare organizations have not conducted a cybersecurity drill with an incident response process despite the frequency of healthcare data breaches.

"The first week I was here, before I even got my feet wet, we were hit by ransomware on one of the computers," said the CIO of a critical access hospital in the Midwest. "And it opened everybody's eyes to our deficiencies in both protecting ourselves and recovering. Now we are aggressively backing up our system, so that if something would happen again, we would be very minimal in time loss."

STRENGTHS AND DEFICIENCIES OF TRADITIONAL BACKUP AND RECOVERY METHODS

Traditional data protection strategies such as archiving, backup and offsite disaster recovery remain popular means of protecting data today. However, the sophistication of today's cyber-criminals has exceeded the ability of traditional data protection and disaster recovery strategies to protect the most critical and valuable data within your healthcare organization.

Data backups, or duplicates of PHI, PII and any other essential data on tape or discs, are vulnerable to cyberattacks – especially from insiders who legitimately have, or who unlawfully gain, access using valid security credentials. This cybersecurity strategy is wholly dependent on how much and how often the organization backs up information, said the CIO of the Midwestern critical access hospital, noting the recovery lesson his organization learned after a ransomware attack occurred during his first week on the job. If the organization does not adequately back up data, it runs the risk of being exfiltrated or forever lost. Furthermore, backups are

> "The sophistication of today's cyber-criminals has exceeded the ability of traditional data protection and disaster recovery strategies to protect the most critical and valuable data within your healthcare organization. "

"Providers need to begin exploring cloud technologies that can be leveraged to plug the gaps and strengthen their data protection and recovery programs."

not immune from the pernicious threat of ransomware. For example, Samas RansomWorm spreads throughout the entire network and encrypts every server, system and backup.

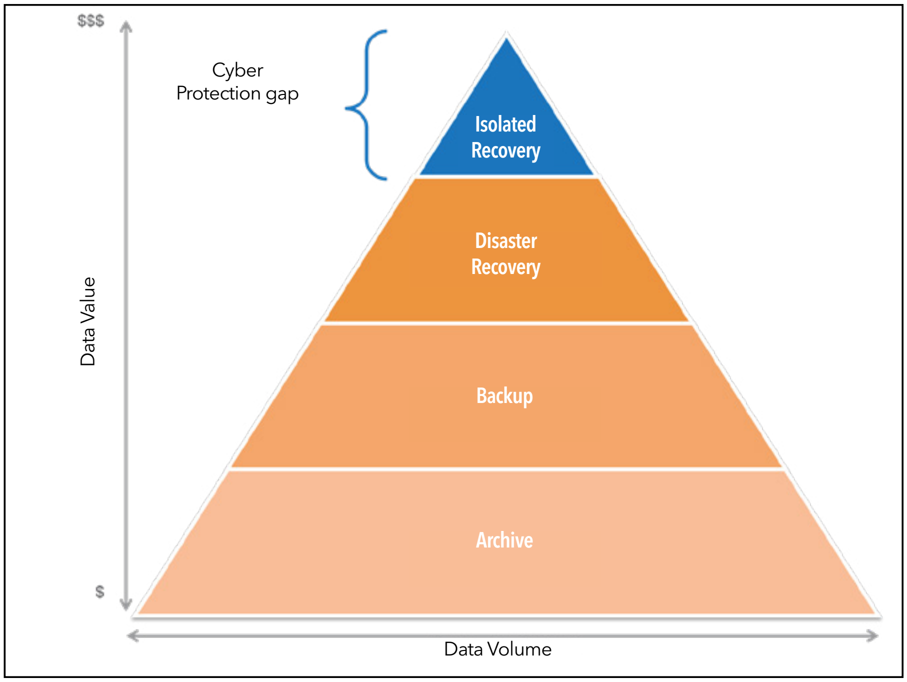
Disaster recovery solutions can be effective protection in the event of a natural or manmade disaster, but still leaves business vulnerable to insider attacks. It can also prove complex and costly to manage multiple data centers and difficult to make the necessary infrastructure available if an outage affects a broad geography.

Backups and disaster recovery are effective to a point in protecting data and critical systems. However, critical systems are still vulnerable to ransomware and other network-based attacks prior to being backed up. Essentially, there is a cyber protection gap left for hackers or insiders to exploit.

A new way of thinking is required to protect critical applications and data that healthcare providers rely on. At the most foundational level, providers need to begin exploring cloud technologies that can be leveraged to plug the gaps and strengthen their data protection and recovery programs. "I would definitely change the way we look at cloud, and move some of our critical services [to] cloud environments that are inherently more resilient," said the chief information security officer of a 200-bed hospital in the Northeast.

To truly elevate cyber-resilience, providers need to expand their pyramid of protection (see Image 1) to include a deliberate and strategic approach to protect and recover the organization's most critical data in the event of a cyber-attack. This is where isolated recovery comes in.

Image 1: Pyramid of Protection



Isolated recovery is a data protection solution that complements disaster recovery and backups by providing an additional layer of security specifically for the most critical data and digital assets. With isolated recovery, PHI, PII and other valuable data are replicated and a second copy is stored in a secure cloud or secure data center offsite. Then, the recovery system in that offsite cloud or data center is disconnected from the network so the data cannot be accessed either remotely or locally.

Isolated recovery's disconnection from the network creates logical isolation. Healthcare organizations frequently update the data stored in the secure offsite cloud or data center and then, should they ever need to recover data due to a cyberattack destroying or compromising their most critical data, they can do so knowing the data has not been accessed by the cyberattacker. Essentially, the isolation of the network prevents the likelihood of hackers manipulating or corrupting the offsite data.

"If there is an event where data gets corrupted or encrypted and you have an environment with redundancy across data centers and data being replicated in almost real time – that corruption or unintentional encryption is going to replicate in real time, defeating your redundancies," said the CISO of the 200-bed Northeastern hospital.

CRITICAL CONSIDERATIONS FOR DELIVERING A BALANCED CYBER RESILIENCE STRATEGY

The number of successful attacks and significant disruption organizations face post-attack are reasons for CISOs to question an approach to cybersecurity that is cyber-prevention-heavy and cyber-recovery-light. In fact, cybersecurity experts and leaders within regulated industries, such as healthcare, financial services and government, now urge businesses to evaluate isolated recovery strategies; especially considering the growing threat cyberattacks, malware, ransomware and insider attacks pose to an organization's livelihood.

SIX KEY TAKEAWAYS FOR CISOS:

- √ Cyber resilience helps mitigate unplanned operational downtime, data loss and destruction.
- √ The risks of cyber attacks and compromise are elevating cyber resiliency to the executive level. Increasingly, healthcare providers are organizing executive-level groups to design and test systemwide recovery plans and capabilities.
- √ Isolated recovery is a critical component of a layered data protection plan, meaning it augments conventional methods like backups and disaster recovery.
- √ To be effective, recovery plans and procedures should be updated and tested regularly.
- √ Best practices for healthcare organizations include the use of dedicated private networks, encryption of in-flight and at rest data and physical isolation of critical data from the network.
- √ If considering a managed service for data protection, look out for additional charges for functions excluded from the monthly fee. These expenses can drive up the cost of the program and render it unsustainable.

Cyber resiliency solutions like isolated recovery help mitigate unplanned operational downtime, data loss and destruction caused by ransomware. Combined, these consequences contribute to reputational damage, costs and lost revenue. The director of network and infrastructure security with a national hospital operator said timing is not only a significant determinant of how much damage an organization incurs after a cyberattack, but timing is also the most difficult factor to control. "The ability to be able to adapt and really respond in a quick manner is the biggest challenge," he said.

One doesn't have to look far to find examples of organizations that experienced unplanned operational downtime over the past several years as cyberattacks overpowered their resiliency capabilities. In 2018, a ransomware attack against one Ohio health system was debilitating enough to disrupt computer systems and force the emergency department to divert patients to other hospitals. A $5 billion health system in Washington, D.C. was locked out of its systems for days. In California, a health system and medical group lost two weeks of clinical information for nine medical centers after a ransomware attack forced reversion to a failed backup system. The incident affected more than 5,000 patients.

The good news is organizations are paying attention and learning from one another. Several participants noted that their organizations have updated cybersecurity strategies in the past three to four years to better account for recovery and resiliency. Take the CIO from the Northeast, who described the leadership, technological solutions and processes his 23-hospital system allocated toward resiliency in 2014, elevating it from a concern for CISOs to a strategic priority for the system's executive and governance bodies.

"We have an executive-level group charged to really be the oversight group for our recovery capabilities," he said. "That group comprises people from many different departments in the health system: corporate communication, legal, IT, compliance, senior administration, corporate security and a number of others. They oversee everything, from technological recovery capabilities all the way to how we manage a problem with PR, regulatory reporting, communications or business associate interactions."

The CIO said the system added technology to its layered defense, including isolated recovery. "We have a copy of our corporate EMR that we store offline, off-network, completely secluded," he said. "If our normal backups become problematic, the offline copy is something we know is good and we can bring it back."

The isolated recovery capability is but one component of the Northeastern health system's layered IT security, augmenting conventional methods like backups and disaster recovery. The cost of isolated recovery means the CIO and his team must be judicious in how it is leveraged across the 23-hospital system. "We can't have that in place for every system – it's cost prohibitive," he said. "So, we do rely a lot on an appropriate DR plan and system recovery plans. We and most places still rely heavily on our backups to be able to recover."
The CISO of the 200-bed hospital in the Northeast said his organization has also integrated isolated recovery into its cyber defense for mission-critical systems for which the organization cannot risk experiencing unplanned operational downtime.

"Every time we do a recovery, whether it's because of a ransomware attack or just a routine recovery, we have built-in encryption that allows us to validate the integrity of the data," he said. "We're doing it only for mission-critical systems that cannot be down, and Air Gapping systems have helped us a lot in preventing corruption from traveling from one system to another."

The CISO is abiding by a best practice by performing routine recovery checks. Disaster recovery plans and recovery procedures should be updated and tested regularly. For the best possible chance of a successful recovery, and to help avoid further infecting the environment after a successful attack, the ability to test and validate fail-safe copies offline and in a secure dedicated environment is an added benefit.

While storing and archiving data remotely is another best practice, corporate networks and public internet links remain susceptible to both insider threats and external hacks. Adding an additional layer of security by using dedicated private networks, encrypting data both in-flight and at rest, and disconnecting the network to provide physical isolation of critical data are emerging best practices for healthcare organizations.

Finally, if considering a managed service for data protection, data archiving or isolated recovery, health IT leaders would be well served to look out for additional charges for data egress, recovery testing and other services excluded from the standard monthly fee. These expenses can drive up the cost of the program, thereby rendering it unsustainable.

CONCLUSION

Although organizations may have robust cybersecurity programs with innovative prevention tools, hackers continuously find new vulnerabilities to exploit. It's time for health systems to meet these new threats with a modern line of defense.

As much as hospitals have invested in cybersecurity and prevention, few are able to fully bounce back from a cyberattack or insider compromise in the desired timeframe. Of the nearly 40 percent of healthcare organizations that have experienced a cyberattack, more than half took several days to restore data to a solid state, according to an IDG-Iron Mountain survey. Until they did so, 65 percent of organizations had to revert to data versions that were days or weeks old. Delays like this bring significant costs for healthcare organizations incurred in a variety of ways, including patient churn and reputational damage.

Organizations safeguard themselves and their patients when they build cybersecurity strategies that balance the focus on prevention and resilience. Although backup and disaster recovery are traditional approaches to cybersecurity, they are still valuable components of a layered defense strategy. Isolated recovery, however, is the next chapter needed to elevate cyber resilience and protect healthcare organizations from experiencing disruption to their business operations, IT downtime and erosion of reputation and patient trust.

> "Adding an additional layer of security by using dedicated private networks, encrypting data both in-flight and at rest, and disconnecting the network to provide physical isolation of critical data are emerging best practices for healthcare organizations. "

MORE INFORMATION

Contact Iron Mountain at 800-899-IRON or visit ironmountain.com/healthcare.

Follow us on Twitter: @IronMtnHealth

Subscribe to our Blog Series: www.infogoto.com/category/industry/healthcare/

IRON MOUNTAIN®

800.899.IRON | IRONMOUNTAIN.COM

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM), founded in 1951, is the global leader for storage and information management services. Trusted by more than 220,000 organizations around the world, and with a real estate network of more than 85 million square feet across more than 1,400 facilities in over 50 countries, Iron Mountain stores and protects billions of information assets, including critical business information, highly sensitive data, and cultural and historical artifacts. Pro-viding solutions that include secure storage, information management, digital transformation, secure destruction, as well as data centers, art storage and logistics, and cloud services, Iron Mountain helps organizations to lower cost and risk, comply with regulations, recover from disaster, and enable a more digital way of working. Visit www.ironmountain.com for more information.