Petri IT Knowledgebase Resource
A BWW Media Group Brand

Petri IT Knowledgebase

Overcoming the 7 Critical Challenges Facing Healthcare IT Today

Sponsored by

Acronis

CONTENTS

The healthcare industry is undergoing a massive transition and the role of IT is expanding given a flood of pressing new challenges. Because of the potential impact on people's lives, new security exploits like ransomware have made data protection and security more important than ever. Meanwhile, the rapid adoption of cutting-edge technologies like artificial intelligence (AI), machine learning (ML) and the Internet of Things (IoT), as well as HIPAA and other compliance requirements creates unique challenges for healthcare IT professionals today.

There's no question that IT needs to step up its efforts to build secure, flexible, mission-critical systems and enable transformation and innovation while meeting new customer needs. Let's take a closer look at the eight critical challenges facing today's healthcare IT organizations and explore how to overcome them.

1 Addressing data breaches, a top issue for healthcare

Data protection and security remain a top priority for today's healthcare organizations. In their study of healthcare data breeches, cybersecurity firm Protenus found that the pace of attacks was more than one breach per day in 2017. The same year, 5.6M patient records were breached – and it took an average of 308 days for an organization to discover the breach occurred.

While external attacks are clearly a major concern, insiders cause the most data breaches in the healthcare industry, according to the HIPAA Journal. As Figure 1 shows, the primary cause of healthcare data breaches is unauthorized access or disclosure of data, followed by hacking or IT incidents.

Advice

To prevent data breaches, you need to have layers of security around your entire IT infrastructure, including physical systems, virtual machines (VMs), cloud services and mobile devices. In addition, you need antivirus

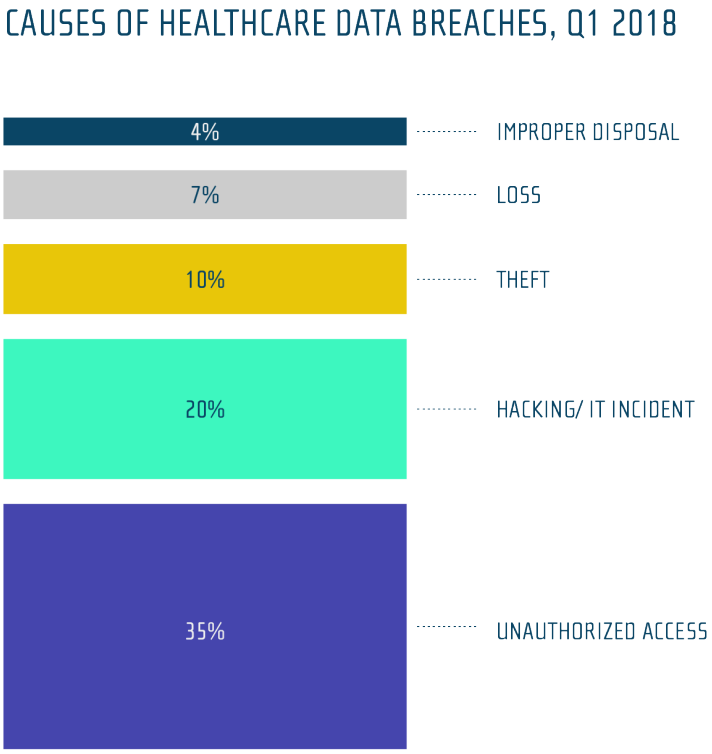

Figure 1- Causes of healthcare data breaches in 2018

protection on endpoints, edge protection using firewalls, and network segmentation using vLANs or software-defined networking (SDN). You also need to ensure that you can restore your data. This means you need to secure your backup process at every stage and securely store your backup files.

Be aware, the storage that you choose for your data and backups significantly affects your data security and protection capabilities. Insecure storage, especially low-cost backup storage, increases your risk of a data breach. Insecure backups can also be a weak link in your data protection strategy. Only use secure certified storage or protected cloud storage to minimize breach potential. Using encryption to protect your storage and backups can also be a powerful tool to prevent unauthorized access to your critical healthcare data – and remain complaint.

2 Protecting against the growing threat of ransomware

There's no doubt that healthcare has felt the brunt of ransomware attacks over the past couple of years, placing it at the forefront of the industry's IT challenges. The always-on requirement for healthcare systems makes them targets for attacks like ransomware, which can render required systems and services unavailable.

According to a threat report released by endpoint security firm Cylance, healthcare suffers almost twice the number of ransomware attacks as the next industry:

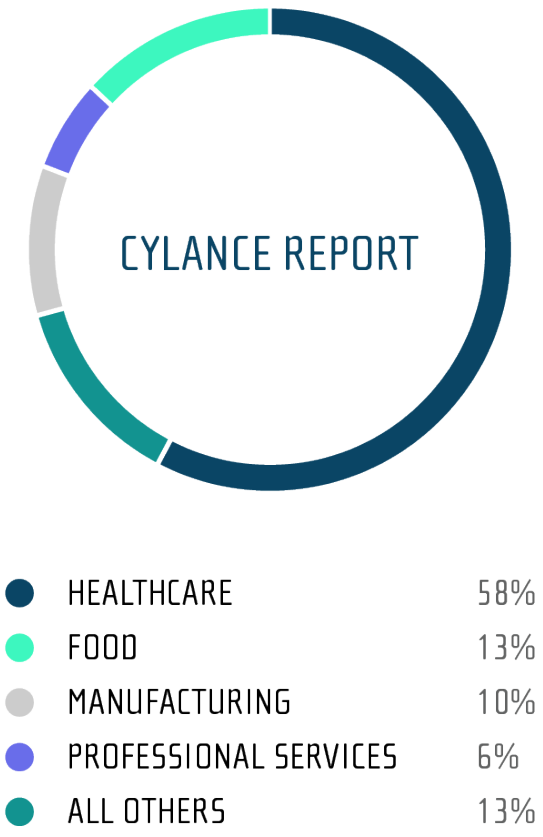

Figure 2 – Cylance report showing ransomware attacks by industry

The Cylance study reveals that 58 percent of all ransomware attacks in 2017 were directed toward healthcare organizations, distantly followed by the food industry at 13 percent, then manufacturing with 10 percent. Ransomware attacks grew three-fold and the healthcare sector was impacted the most. Cylance Worldwide CTO Rahul Kashyap stated, "It's critical that companies are aware of the threats, keep up-to-date with patches, and use defenses that protect against constantly evolving malware."

> **"It's critical that companies are aware of the threats, keep up-to-date with patches, and use defenses that protect against constantly evolving malware."**
>
> **Cylance Worldwide, CTO,** Rahul Kashyap

Verizon's 2018 Data Breach Investigations Report (DBIR) also showed that ransomware attacks are on the rise, particularly for the healthcare industry: ransomware accounted for 85 percent of malware attacks. The Verizon study showed that employees continue to fall victim to social engineering attacks. Financial pretexting and phishing represented 98 percent of social incidents and 93 percent of all investigated breaches – with email continuing to be the main entry point. Per the Verizon report, "Preventive controls regarding defending against malware installation are of utmost importance."

Advice

Traditional signature-based anti-viruses are not designed to fight ransomware and other zero-day threats. Only new AI- and ML-based countermeasures can recognize malicious behavior, prevent harmful effects, and even automatically restore data.

Backup solutions themselves also require tight, built-in security measures to enable better business continuity and protect critical data from threats like external hackers, insider attacks, and a broad array of malware, including ransomware. In fact, some malware threats are able to search for and destroy backup files.

Combatting these threats requires a multi-faceted approach which includes: implementing clear social and email policies; maintaining user-education to prevent the initial infection itself; and using a modern solution that protects your system by actively detecting ransomware and stopping an attack outright.

3 Meeting HIPAA and other compliance requirements by running VMs directly from backups

Healthcare IT involves working with a lot of sensitive and private information that is subject to governmental oversight and regulation, so healthcare compliance is another big challenge that affects every type of provider and organization. These requirements are not going to diminish over time, rather there is every reason to expect they will increase.

The Health Insurance Portability and Accountability Act (HIPAA) is the primary healthcare regulation in the United States. For a healthcare organization to be HIPAA compliant, it needs to ensure that the specified level of data access controls are in place for protected patient health information. HIPAA consists of a set of patient privacy laws that stop organizations from disclosing and sharing medical data.

With more than 186,000 privacy rule complaints recorded since 2003 according to HHS.Gov, there's no doubt HIPAA compliance is a challenge for healthcare IT. Noncompliance has cost healthcare organizations millions of dollars in fines.

To make sure your organization is HIPAA compliant, you must ensure that your data protection systems can meet the five essential HIPAA security standards. Designed to be technology-neutral, HIPAA doesn't require you to use specific technologies. However, the technologies you implement need to ensure:

- **Access control.** Specifically, you must be able to assign a unique identifier to patients, implement procedures that terminate an electronic session after a specific period of inactivity and implement a mechanism to encrypt protected health information.
- **Audit controls.** This means your solution must be able to deploy procedural mechanisms that record and examine the activity in information systems.
- **Data integrity.** Built-in mechanisms should ensure that unauthorized activity has not altered or destroyed protected health information.
- **User authentication.** Anyone seeking access to protected health information must be who they claim to be.
- **Transmission security.** All electronically-transmitted personal health information should be encrypted and must be unaltered by an illegitimate source.

Advice

In order to comply with HIPPA regulations, you need to review your organization's personal data usage and understand how the data is being processed, stored, transferred and shared, both inside and outside of your facilities. You also need to determine if your organization is capable of detecting and reporting data breaches within the required time window.

To achieve compliance, businesses must conform to rules for managing and securing personal data. Organizations must provide strong data encryption locally, on devices, in-transit and in the cloud. They also need to be able to search for and modify personal data (if specifically requested by a patient) online or inside backups as well as provide proof of data integrity.

4 Moving to the cloud

Nowadays cloud technology is a core component for most businesses, and the cloud is impacting healthcare IT systems, too. The cloud improves efficiency by helping to manage (or cut) costs, ensure cost predictability, and

speed up the deployment of new services. It offers a single shared access point for patient information and can enable multiple doctors to view lab results and consult notes.

Cloud software-as-a-service (SaaS) applications can also be used to replace aging legacy on-premise applications, eliminating costly application redevelopment. A 2017 survey by HiMSS Analytics showed that many healthcare organizations were already utilizing the cloud or cloud services – and that the majority of cloud usage was for SaaS applications, as shown in Figure 3:

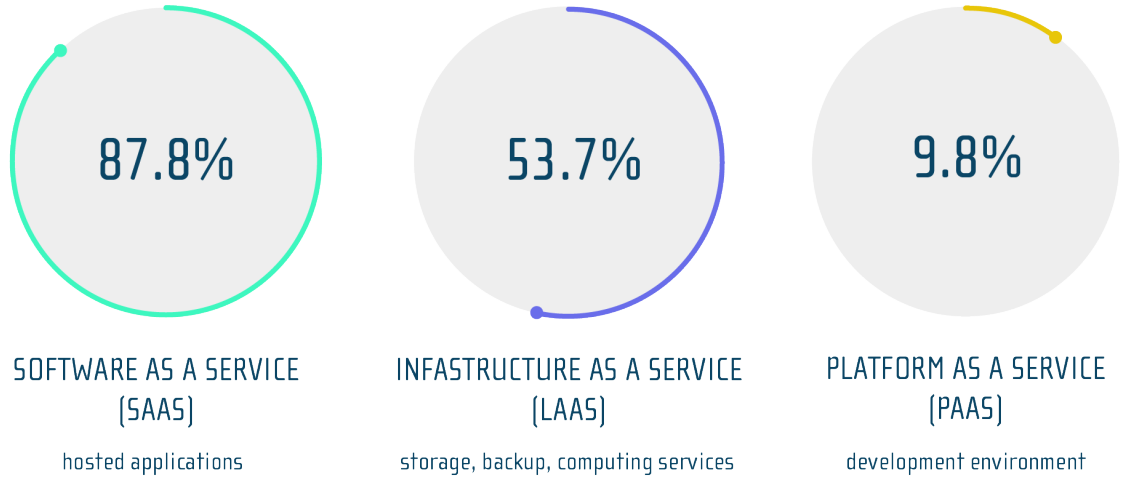

Figure 3 – Cloud usage by healthcare organizations

Figure 3 shows that nearly 88 percent of respondents are using a SaaS model. Infrastructure-as-a-Service (IaaS) usage was at nearly 54 percent, mainly for storage and backup, while using Platform-as-a-Service (PaaS) for development trailed at about 10 percent.

However, moving into the cloud and adopting cloud services can pose several significant challenges for healthcare organizations. First, many in-house IT organizations lack cloud skills, requiring training in new areas such as cloud management and cloud storage methods. Next, migrating data from one storage type to another is no small task for healthcare organizations. In many cases, protected health information that is available. Your IT staff is responsible for ensuring that your organization's sensitive data and critical applications are protected.

Before moving to the cloud, you need to:

- Make cloud training available for your IT personnel so they can understand and effectively manage your cloud solutions
- Select data protection solutions that will not disrupt physician or staff workflow
- Be sure your data protection solution works for local, hybrid and cloud data
- Assess your healthcare applications and data to determine an effective and secure migration strategy in which all migrated data is encrypted and secured during the migration process
- Confirm that your cloud storage and backup strategies are secure and compliant: they must support authentication, encryption, portability, and integrity as well as providing fast recovery times

5 Delivering constant availability of data with quick restore capabilities

High and continuous availability of data and systems

are vitally important in the healthcare industry because patients' well-being (and sometimes even their lives) depend on it. Even so, all systems are subject to failure for a variety of reasons. Working to ensure your data is protected and secured even in the event of a failure is essential.

Organizations studied by the Ponemon Institute in its Benchmark Study on Privacy & Security of Healthcare Data, indicated that there is a definite gap in healthcare organizations' confidence and ability to detect and respond to incidents and data loss and restore data. Their 2016 report on the cost of data center outages showed that the average cost of a data center outage was $740,357 and that costs had increased 38 percent since 2010. The average cost per minute was $8,851 per incident. Meanwhile, the average per-incident cost of unplanned outages for the healthcare industry was $918,000. While the monetary costs of downtime are very high, there can also be significant consequences regarding patient safety and the delivery of patient care.

"$918,000 was average per-incident cost of unplanned outages for the healthcare industry."

To ensure the ability to restore your data, it is essential that you understand your Recovery Point Objectives (RPOs) and Restore Time Objectives (RTOs). To know your RPOs, you can ask how much data your organization can afford to lose. Likewise, to determine your RTOs, you can ask how long your organization can run without its critical data. Knowing your RPO and RTO requirements will help you to understand the data protection and recovery technologies you need.

Advice

To effectively protect and restore your data, you need to be able to select several different points in time for data restoration. Your data protection solution needs to protect you from downtime by proactively stopping malware and ransomware attacks and automatically restore data in case of an attack. You must be able to quickly restore your backup data. For instance, if you have a server failure, most backup solutions require you to restore your backup to identical hardware, which will significantly increase the time needed to restore your data. For rapid recovery, you need maximum flexibility t to restore your workloads to the cloud, to a new virtual machine, or to dissimilar hardware. The versatility of restore operations with increased speed and flexibility could save someone's health or career.

6 Incorporating mobile devices

The incorporation of bring your own device (BYOD) mobile devices is another big challenge for healthcare organization today what with the growing trend of consumerization in the workplace. For example, patient information is now being collected and made available on a variety of mobile and web-based devices. To further enable mobility, enhance productivity of staff, and control costs, many hospitals are embracing a BYOD strategy that includes smartphones, tablets and hybrid laptops. (Employees also tend to like it because they only have to carry one device with them and they are familiar with how to use it.)

For the healthcare industry, however, BYOD brings with it several important considerations. BYOD devices are inherently less secure than company-supplied devices. According to the U.S. Department of Health and Human Services, the number one cause of data breaches is device theft, which can enable unauthorized access to confidential and private healthcare information.

Advice

A BYOD strategy needs to be coupled with strong device management policies that govern usage and data protection. You need to be sure that mobile devices are equipped with strong authentication and access controls. For device-level protection, your mobile devices must support encryption and you need to protect all wireless transmissions from intrusion. It is unwise to transmit unencrypted, protected health information across public networks. Remote device data needs to be backed up, and those backups need to be

secured with encryption. In addition, all mobile devices used for healthcare should support policies that enable remote device wiping and remote disabling.

7 Strengthening data protection without adding infrastructure complexity

Your data protection solution must not require rocket science to run or add costs or complexity to your infrastructure. Rather, your IT generalists need to be able to effectively and efficiently use it to protect and quickly restore your data. Using multiple tools increases the risk of errors for both backup and restore operations, increasing downtime as well as data exposure and data loss.

Advice

To simplify data protection for your healthcare organization, you should have one tool that can protect all of your workloads and manage storage, retention, backups, and restoral operations. It should be able to protect your local workloads as well as workloads in the cloud and on your mobile devices. This tool should be easy to learn and should be able to scale with your data protection needs. You should not need to replace your data protection solution just because you add another cloud application or more storage. Your data protection should not limit your growth or ability to adopt new IT infrastructure. It should provide secure storage, backup encryption and rapid point-in-time recovery.

Final Thought: Acronis can help solve your healthcare IT challenges

Healthcare IT organizations face a wide array of challenges in today's complex, evolving and increasingly threatened landscape. Acronis Backup, Acronis Storage and Acronis Cloud Storage can help organizations address these issues and meet HIPAA and GDPR compliance requirements with the level of data protection and security healthcare organizations require today.

Acronis Backup provides fully encrypted backups with the ability to search them as well as rapidly recover complete systems from backups within minutes. Built-in ransomware protection prevents data corruption while the use of blockchain ensures the integrity of your backups. For additional backup data protection while maintaining full control on data sovereignty, Acronis Backup can also replicate archives to Amazon Web Services (AWS), Microsoft Azure, Google Cloud Storage or another remote data center. It also provides built-in deduplication and adaptive compression. Data encryption support protects your data at rest and enables you to change passwords without requiring re-encryption.

Acronis Active Protection uses AI- and ML-based technology to protect all executables and data (e.g. documents, media files, programs, and Acronis backup files) from ransomware attacks. This advanced, proactive technology is integrated into Acronis Backup and prevents system unavailability caused by 99.99 percent of ransomware. Better still, any files impacted before an attack was stopped are automatically restored from an Acronis-protected backup archive.

Acronis Cloud Storage is an easy-to-use, off-site cloud backup storage option that is fully integrated into Acronis Backup. Acronis data centers are HIPAA compliant and provide multiple storage options to make compliance easier.

Acronis Universal Restore and **Acronis Instant Restore** facilitates fast and flexible restore operations. Acronis Universal Restore eliminates the need to restore backups to identical hardware by allowing you to restore backups to different physical, virtual or cloud systems. It reconfigures the target operating system before booting, changes any required OS settings, and injects any drivers required to boot the system. Acronis Instant Restore enables you to vastly reduce recovery times by using your backups to immediately start

VMs directly from storage. In addition to fast, flexible data recovery, Acronis bootable media also provides the ability to mass-image computers. Bootable media enables you to run Acronis Backup and recover on a system without needing the OS. You can use it with your backups to create images, clone hard disk drives, and partition new hard disk drives.

There is no doubt that the most important attribute for your data protection tools is reliability – you have to trust that your backup vendor safely stored your data and that it can be recovered quickly. Acronis ensures that your data is secure and that you can remain compliant, while its ease-of-use and wide range of protection capabilities help to simplify your IT operations.

Acronis