HEALTHCARE DATA BREACH TREND REPORT 2021

How are cybersecurity teams, healthcare organizations and law enforcement agencies preparing for the biggest cyber risk to hit our health system in 2022?

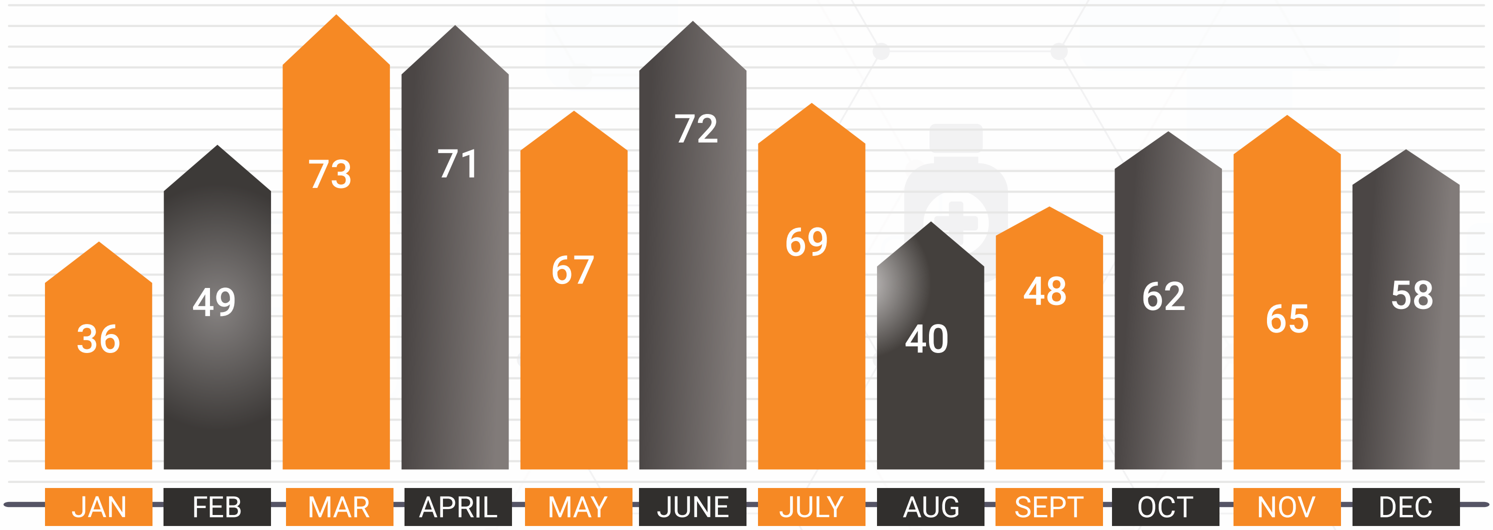
PROTECTED
HARBOR

INTRODUCTION

Digital healthcare services supported by the internet, information systems, and smart devices have revolutionized the health industry and made it easier for people to access treatment. Electronic health records (EHRs) have replaced paper-based systems leading to the faster and more efficient delivery of healthcare services. In addition, digital technology has enhanced how healthcare providers communicate among themselves and with patients. This is evidenced by the success of healthcare technology such as mHealth, telehealth, and telemedicine in facilitating patient management. These technologies have empowered patients and allowed them to access healthcare information online conveniently. It has also improved patient data collection, including personal data, stored in hospital network servers for future reference. While EHRs have revolutionized modern healthcare delivery, they are a liability to the healthcare industry due to software vulnerability, human error, and security failure.

Technologies' vulnerability has continuously exposed healthcare data to external and internal data breaches. The most prevalent forms of attacks on healthcare data include hacking or IT incidents, unauthorized access and disclosure of data, theft, and loss of data. Healthcare data is regarded as valuable and, hence, a major lure for misappropriation and hacking. Recent data shows that the frequency of malicious attacks and illegal disclosure of healthcare data has risen by 162% in the last three years. In 2021 there were over 700 healthcare data breaches affecting many people including patients. The incidences have not only been a concern to security experts but also to the various healthcare stakeholders including patients and hospitals. This is because tampering with healthcare data may lead to wrong diagnosis and treatment, contributing to fatal outcomes. Many hospitals lack the resources to protect themselves from these malicious attacks leading to data loss, financial loss and access to sensitive data by unauthorized persons.

BREACH BY SUBMISSION DATE



CURRENT STATISTICS & TRENDS

Research shows that hospitals account for about 30% of all large data breaches in the United States. The huge cybersecurity spending of about $65 billion between 2017 and 2021 corresponds to recent data indicating a growth in healthcare data breaches. Since 2009, more than 2100 healthcare data have occurred, indicating that the healthcare industry faces the highest number of cyberattacks and data misappropriation across all industries. On average, about 59 data breaches were reported every month in 2021, with 710 breaches reported for the entire year. More than 1.5 million records were affected across 39 breaches to healthcare data in February 2020. Compared to 2021, the months of March, April and June saw the highest number of breaches reported, with an average of 72 data breaches in each of the three months.

The total number of breaches may have been more than reported, considering research shows that between 60% and 80% of data breaches are usually unreported. The US laws require that covered entities report breaches involving 500 or more individuals to the HHS. Independent hospitals may experience data breaches, but the covered entity they work for reports braches separately. For example, the California Department of State Hospitals (DSH) is a covered entity that has five hospitals under the organization. Any of the five independent hospitals can experience data breaches but only DSH reports the breaches.

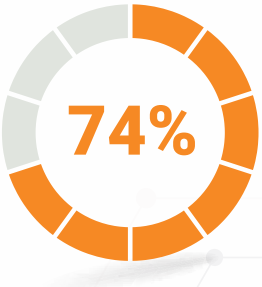
Cybersecurity breaches on healthcare records threaten patients' identity and finance and present a stabling block to the efficient operations of hospitals. Attacks such as ransomware forces healthcare providers to delay treatment plans, which impedes the well-being of at-risk patients. Data shows that healthcare data breaches affected more than 40 million records compared to 26.4 million in 2020. Some notable cybersecurity breach cases in 2021 exemplify the magnitude of these attacks on patients and healthcare organizations. A phishing attack at the Florida Healthy Kids Corporation in June 2021 exposed personal and financial information, affecting 3.5 million individuals. In July 2021, the Forefront Dermatology organization reported a cybersecurity attack on its IT systems, leading to unauthorized patient and employee personal information access. This attack was reported to have affected more than 2.5 million individuals.

Research shows that estimating the actual costs of data breaches in the healthcare industry is a challenge due to insufficient data and a huge number of unreported cybersecurity attacks. The affected organization can incur costs in two phases. Immediate costs are incurred when responding to cybersecurity attacks and long-term costs to the overall business due to the attacks. Some costs related to data breaches are unavoidable and easy to quantify. Other costs are intangible relating to the nature of the breach and these costs can spread over a number of years. Healthcare organizations have an urgent need to effectively estimate costs likely to be incurred in the event of a cybersecurity attack. It is estimated that the US healthcare industry is likely to incur $7 billion annually from lost stole PHI. In 2021, the healthcare industry was estimated to face high financial consequences due to data breaches. According to HIPAA, healthcare data cost the highest across all industries at $408 per record. Overall, cybersecurity breaches cost the healthcare industry $25 billion in 2021 alone. The attacks cost the global healthcare industry more than $6 trillion in 2020.

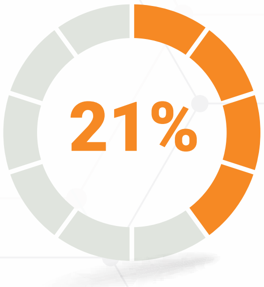
TYPES OF BREACHES

Cybersecurity is significantly under threat with advances in technology and increased use of the internet of things (IoT) in the healthcare industry. Healthcare data breaches are mainly caused by internal or external malicious attacks. They are linked to employees abusing their access or unauthorized external agents exploiting weak credentials and using malware to attack organization systems and access personal data. External incidences dominated data breaches in the healthcare industry. About two-thirds of the data breaches reported in 2021 were related to hacking and IT incidents account for 74% of total data breaches.

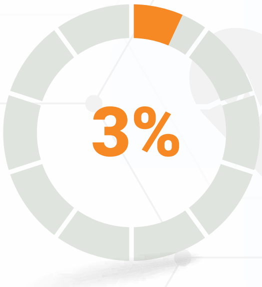
Unauthorized access and disclosure of health records accounted for 21% while theft, loss and improper disposal of healthcare data accounted 5% of total breaches.



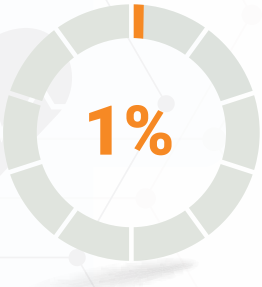
Hacking/IT Incident



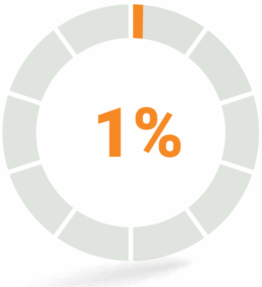
Unauthorized Access/Disclosure



Theft



Loss

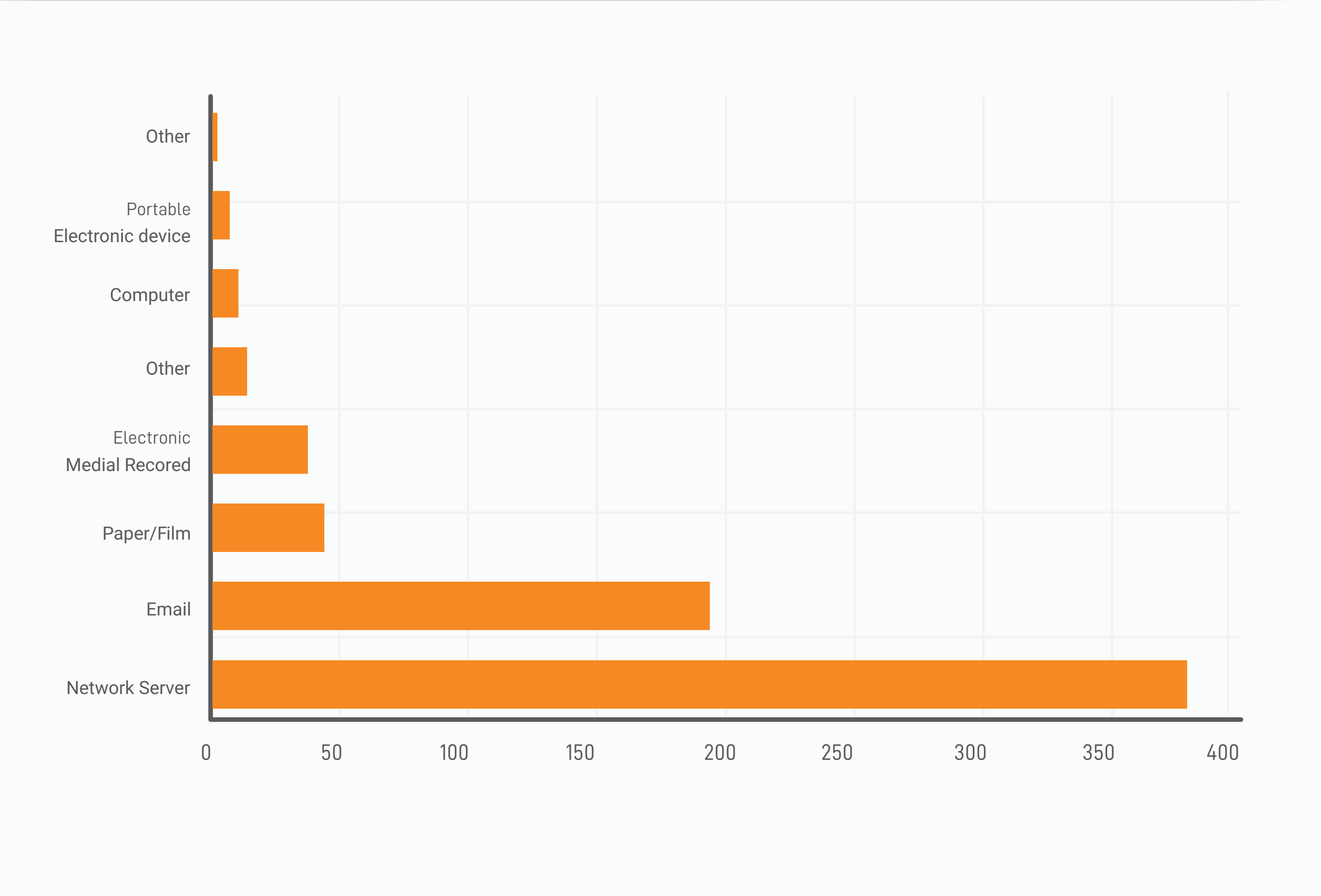


Improper Disposal

The most common breaching points in the healthcare data were network servers and emails and were linked to more than 80% of the total breaches in the entire 2021. Many healthcare breaches start with phishing emails to infect IT systems with ransomware. Hackers find PHI valuable, so they aggressively attack the healthcare industry. Health organizations lack advanced IT systems and cybersecurity software, which increases the vulnerability of the systems to attacks by hackers. The media and also the FBI have highlighted various ransomware variants such as Conti, PYSA, Lockbit and Zeppelin.

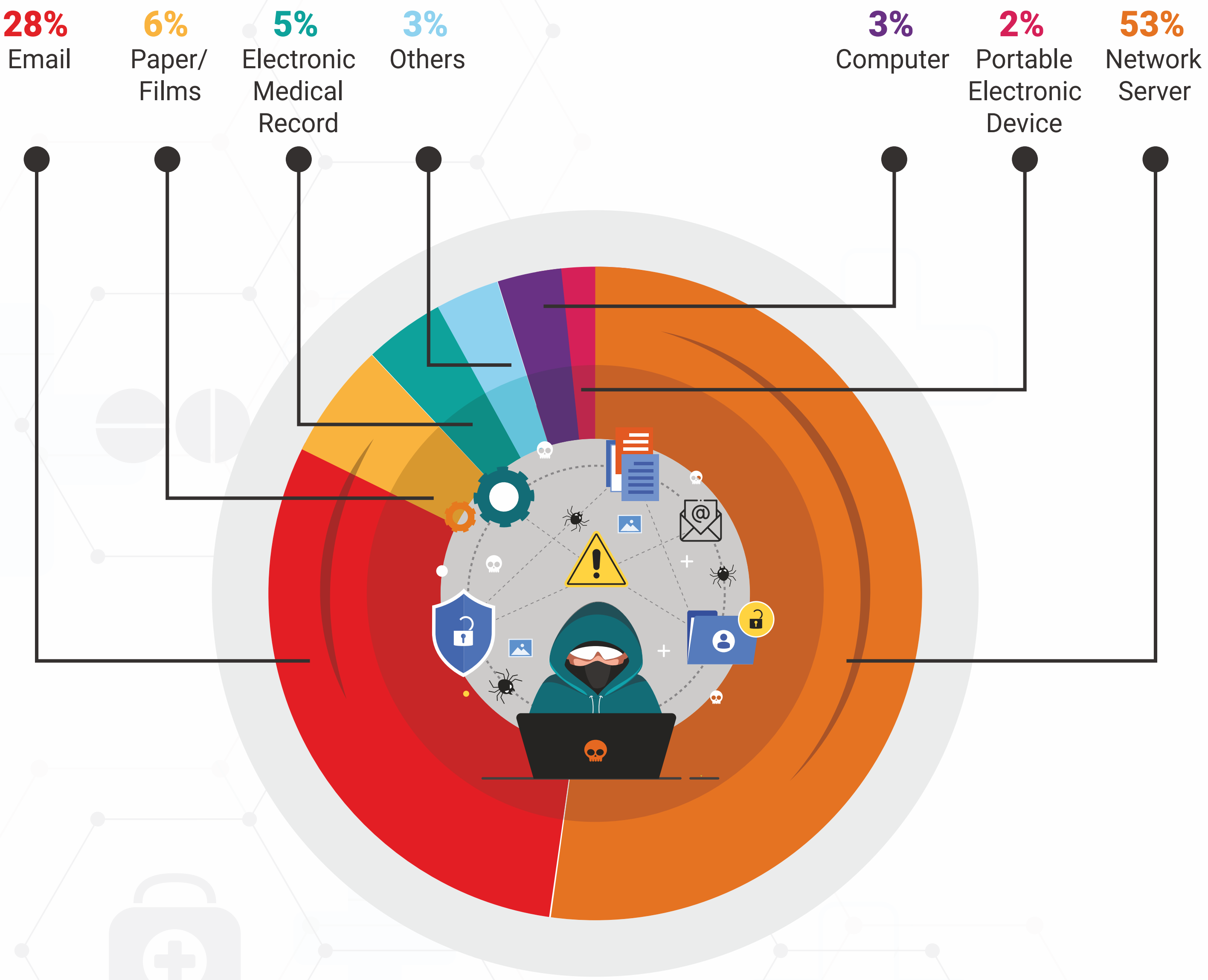
For example, at the Coombe Hospital, the Russian cybercriminal gang gained access to the hospital's systems by sending a contaminated email to an HSE member of staff and affected several IT systems. Similarly, the data breach at St. Joseph's Candler Health System in August 2021 was found to have originated from ransomware and affected the Georgia health systems thus preventing online access to the systems. The hacker had accessed the systems for more than six months. In another case reported in the same month by the University Medical Center Southern Nevada, a notorious REvil ransomware gang accessed the organization's system, compromising the personal and health information of the affected people. The prevalence of external attacks corresponds to facts above that hacking and IT systems-related cybersecurity attacks dominated data breaches in the healthcare industry.

THE WAY IN...



Similar to hacking, attackers access medical information resulting from errors committed by employees or even acts by malicious insiders. Data highlighted other common breaching points such as paper, electronic media records, computers and portable electronic devices which accounted for less than 20% of the total healthcare data breaches in 2021. For example, a data breach at Gale Healthcare solutions reported in December 2021 was found to have occurred due to a non-password-protected database that was easily accessible to the public hence exposing sensitive health information to third-party individuals. A data breach at Telehealth app Doxy.me reported in October 2021 was found to have originated from a coding issue that seemed to share IP addresses and unique device identification with various online platforms including Google and Facebook. The breach allowed unauthorized individuals to access healthcare providers' and patients' information. Healthcare organizations and business associates may be are getting better at protecting healthcare records with physical, technical, and administrative controls but becoming more susceptible to cybersecurity attacks.

THE WAY IN...



The facts mentioned in this report demonstrate the vulnerability of healthcare organizations in this era of advanced technology and the internet of things. Hospitals and patient records are at risk of being accessed and exposed to unauthorized people. Alarmingly, the health industry is being targeted because healthcare data is very valuable. Attackers capitalize on the vulnerability of technology to hack and access patients' personal information which has had significant financial consequences to the victims. In this respect, the privacy and confidentiality of healthcare data is a major concern for patients and healthcare settings. The sensitivity of healthcare data and its importance to patient treatment as well as organization reputation and revenue necessitates the need to enhance the security and protection of the data.

ORGANIZATIONS ATTACKED

Healthcare organizations and businesses associated were faced with cybersecurity attacks and misappropriation of healthcare data in 2021. In April 2021, cybercriminals attacked the Reproductive Biology Associates and my Egg Bank North America affiliate organization. The attackers accessed personal information including medical and social security number information belonging to 38,000 patients. Various media reports have indicated that cybercriminal organizations may be responsible for most of the attacks on the healthcare industry. For example, the notorious REvil ransomware gang was linked to the data breach at University Medical Center Southern Nevada in August 2021 that affected 1.3 million individuals.

Covered Organization	No. of Individual Affected	Breach Cause
Florida Healthy Kids Corporation	3,500,000	Hosting Patch Failure
20/20 Eye Care Network, Inc	3,253,822	Insider Wrongdoing
Forefront Dermatology, S.C.	2,413,553	IT Network Hacked
CaptureRx	1,656,569	Ransomware
Eskenazi Health	1,515,918	IP Spoofing
The Kroger Co.	1,474,284	3rd Party File Transfer Failure
St. Joseph's / Candler Hospital	1,400,000	Ransomware
University Medical Center Southern Nevada	1,300,000	REvil Ransomware
American Anesthesiology, Inc.	1,269,074	3rd Party Phishing Incident
PracticeFirst	1,210,688	Ransomware

THE CHALLENGES

Cybersecurity must adapt to changes in relevant dynamics, including technology and common vulnerabilities. Covid-19 related constraints and new technology present significant challenges for healthcare organizations and expose their vulnerabilities. Cybercriminals are leveraging the increased reliance on technology and the internet to attack and misappropriate healthcare data. This has created fear, uncertainty, and doubt in the healthcare industry. Significant literature has examined the evolution of cybersecurity threats in the UK, US, and Australian healthcare sectors, though limited literature has focused on potential solutions.

Many aspects of healthcare systems have been tested, especially in terms of their overall readiness. However, recent challenges to healthcare systems have served as a catalyst for transformation. Healthcare systems have sped up implementing and adopting public health solutions. This includes integrating patient needs into a new healthcare system framework that emphasizes preventive measures, remote care and includes a substantial reliance on technology. Below are the common challenges that have contributed to medical data and privacy issues in the healthcare industry.

IoT CONNECTED MEDICAL DEVICES

Technology and the advancement of the Internet of Things (IoT) have opened up new possibilities for healthcare. However, these same advances present Healthcare organizations with many challenges.

With an abundance of sophisticated and targeted attacks aimed at penetrating their networks, Healthcare organizations need to take additional steps to protect themselves. Now more than ever, it's critical for organizations to be aware of evolving threats and to implement precautions that keep patient data secure.

Visibility into each device's security posture and network status, location, and device usage remains a challenge for IT professionals. How do you know what devices are on your network? What are they doing? Where are they? What is their status? A lack of centralized control over IoT devices can make managing them difficult. How do you manage them if you can't see what is happening or where devices are located?

According to a report, spending on medical devices with internet connectivity is expected to grow at a CAGR of 29.5% through 2028. Patient monitors, ventilators, and IV pumps are among the 15 to 20 connected medical devices in the standard hospital room. These Internet of Medical Things (IoMT) tools have become an essential element of patient care, while also posing security risks.

mHealth AND TELEHEALTH TECHNOLOGIES

Another rising demand and external access point that can be difficult to control is providing healthcare remotely. Mobile Health (mHealth) and Telehealth Technologies are transforming medicine and giving patients more access points for care, but increasing access increases the risk for breaches. In 2017, almost 1,500 data breaches were reported to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR). Thirty-five percent of those breaches involved a mobile device or portable media. This number is only expected to grow as mHealth apps become more widely used by physicians and patients alike.

If significant privacy and security problems are not addressed, telehealth's success may be jeopardized. For example, sensors used to detect safety issues or medical emergencies may inadvertently broadcast sensitive information about household activities. Providers and patients will lose trust in telehealth solutions if the underlying data and technologies do not have proper security and privacy protections. Best practices for data privacy and telehealth include strong authentication, end-to-end encryption, appropriate technical control, and adherence to best practices.

> ***“We need a cost-effective, high-quality health care system, guaranteeing health care to all of our people as a right.”***
> *Richard Luna, CEO, Protected Harbor*

CURES ACT & PATIENT ACCESS

The Cures Act requires easy patient access to their medical records whenever and wherever they need them. But this is an unprecedented vulnerability in terms of privacy and attack. How do you secure patient information wherever and whenever they require it?

New federal laws supported by the twenty-first Century Cures Act requires organizations to provide patients with quick access to their healthcare data and guarantee that patients will be able to share their electronic health data (EHI). Healthcare organizations that do not implement systems that support patient access or that have inoperable systems could be liable for fines and penalties. Interoperability reduces the burden of administration but also presents an unprecedented vulnerability in terms of privacy and attack.

UNDERSTAFFED & UNDERFUNDED IT DEPARTMENTS

The healthcare industry has made enormous strides over the past few years to embrace the value of technology and leverage it to improve the experiences and outcomes of patients. But while these advancements have been game-changing, they've also increased the risk of cybersecurity attacks.

Healthcare organizations have a lot on their plates right now. They're focused on implementing new technologies, adjusting to changes in payment models, and complying with new standards. And in many cases, they're doing all this with limited resources.

It's no wonder that 55 percent of healthcare organizations report fewer than ten full-time employees dedicated to IT security, compared with 24 percent in other industries. And with more than 90 percent of healthcare organizations using cloud or hybrid environments — compared with 82 percent elsewhere — this understaffing is particularly risky.

The growing burden on IT staff is a significant challenge that has already been identified by cybersecurity professionals in healthcare organizations. A majority of IT departments are still understaffed and overburdened with day-to-day work. This leaves little time for them to improve their security infrastructure, as they are always reacting rather than improving. It doesn't help that majority of their time is spent on manual tasks like creating tickets, which could easily be automated.

LACK OF EMPLOYEE SECURITY TRAINING

In a world where data breaches are common, it's vital for employees to know how to spot suspicious emails, lock-up devices with sensitive information, and more. Unfortunately, many healthcare providers have failed to adequately train employees on the basics of IT security.

Analysts claim that non-malicious attacks are the most common security breaches that healthcare organizations face. A study by the Ponemon Institute showed that 47% of non-malicious attacks were caused by employee negligence, while 29% were due to system glitches, and 24% were because of third-party errors.

I believe health care is a civil right.

If 91% of cyber-attacks start with an email and 24% of physicians can't identify phishing emails, then it is only a matter of time. The first step to combating this threat is to educate employees on how to recognize potentially malicious emails. Employees should also be trained on the importance of strong passwords and other security precautions, such as not leaving laptops or mobile devices unattended in public places.

REGULATORY

When collecting health information, health-focused IT companies frequently find themselves in a regulatory grey area. Regulatory agencies have not kept pace with technology advancements, leaving some businesses in the dark about health data exchanges' regulations. The Office of the National Coordinator for Health Information Technology (ONC) aims to issue the final version of the Trusted Exchange Framework and Common Agreement (TEFCA) in the first quarter of 2022. Qualified Health Information Networks (QHINs) will begin signing the Common Agreement by the end of 2022. There are presently no industry-wide standards for trusted data exchange. TEFCA will provide the infrastructure architecture and governing strategy for users in various networks to securely share basic clinical information while adhering to commonly agreed-upon expectations and regulations, independent of which network they are in. Until that time comes, the industry will be flying blind.

DARKWEB

The dark web is a haven for cybercriminals. This is where they buy and sell stolen credit card information, login credentials, and even copyrighted material such as Netflix's proprietary software. It's also where they advertise their services — everything from spear-phishing campaigns to ransomware-as-a-service.

The apparent increase in demand for medical data on black market sites is also troubling because it suggests that it is more valuable than other personal information such as credit card numbers. On average, the cost of acquiring one piece of health insurance-related information is $20, while one credit card record averages $7.50.

Additionally, we are seeing an increase in sophisticated hacking tactics, such as remote access Trojans and phishing campaigns, which are explicitly targeting healthcare organizations. It seems that healthcare organizations are not keeping up with security advancements that have been made in other industries, leaving them open to attack.

Cybercriminals use the dark web to communicate because it offers a high degree of anonymity. The dark web incentivizes cybercriminal activities on healthcare data, which is considered very valuable. As the covid-19 vaccine rollout continues, expert and media reports have shown increased demand for health data such as covid-19 test results and vaccination records in the dark web. A special report by US drugmaker Pfizer and German BioNTech stated that documents related to their vaccine development were unlawfully accessed from the European Medicines Agency (EMA) and manipulated before they were leaked to the dark web. This poses a threat to the vaccine supply chain and may delay the delivery of the vaccines.

THE PLAYBOOK

The rapid advancement in technology has led to the rise in demands for secure environments for data exchange in various sectors, including health care. Server security covers tools and processes that help safeguard valuable assets and data residing in the company servers, among other accompanying server resources. Due to the sensitivity of the data in servers, they are a major target of cybercriminals who are constantly looking for ways to exploit and take advantage of the innovation vulnerabilities. Servers sit at the core of a company's IT framework and allow numerous users to obtain similar data and operations remotely and simultaneously. Operating system patching in a server environment helps establish a secure system through the prevention of malicious hackers who exploit any existing vulnerabilities that in the long run reduce the risks of an attack. Ensuring that a firewall is always enabled ensures optimum defense against suspicious network traffic. User access system access privileges should be as restrictive as possible, thus reducing both intentional and unintended server safety breaches. However, failure to keep the firmware and drivers always updated can lead to significant business losses.

The increased application of e-health and telehealth has enabled health organizations to discover the need to place their data and workload records in private cloud networks due to their increased security. Achieving this requires IT specialists to develop sound designs and frameworks with appropriate network configurations to maximize the application of cloud-based resources. They should also ensure that system designs meet relevant privacy standards, such as HIPAA (the Health Insurance Portability and Accountability Act of 1996) or GRC (governance, risk, and compliance), and avoid violating predefined policies. Service Organization Control (SOC) 1 and SOC 2 certification will guarantee data security and integrity, thus increasing safety in business operations.

Following the below strategies will help in establishing a secure digital platform that integrates legacy technology focusing on speed, security, and uptime.

LEGACY SYSTEM TRANSITION PLANNING

Every application, system, and technology device in the healthcare domain will eventually become obsolete. Health systems will need to develop a bridge program to determine how to manage these devices until they can be replaced. Those hardware and software that have reached the end of life and are associated with known vulnerabilities neither be in the corporate network nor repaired since they are prone to cyberattacks. Healthcare companies should be aware of the date when support will be discontinued, and a strategy for replacing old software and devices should be devised.

Until that time update all software! This should be a rule no matter what technology systems you are using. Different Healthcare organizations use multiple software throughout the organization to perform various tasks. Different versions of the software are released from time to time to reduce the weaknesses and other loopholes in the previous versions.

Keeping all the software up to date is essential for the better performance of the software. It also helps discourage potential cyber criminals who take advantage of previously-found weaknesses in software.

Whenever a new version of the software is released, the software developers inform all users regarding the updates. The IT admins should update all the software and operating systems throughout the organization from time to time to keep their IT system and network security.

CONDUCT REGULAR AUDITS

Auditing is a process of examining how well a healthcare organization's system conforms to an established set of security criteria. It includes assessing the security of the system's physical configuration, information handling processes, user practices, and software.

Conducting regular audits is vital to identify security problems and system weaknesses, establish a security baseline to compare the future audits, comply with internal and external security policies, and identify unnecessary resources. It also helps ensure that any information is being added or updated in the system by an authenticated user, and no one can access the system without verifying their identity.

While performing an audit, system administrators should ensure that the system uses two-step authentication, all users use a strong password, and change it at regular intervals. They should also evaluate the access credentials to ensure that the previous employees do not access the data.

ISOLATE & VALIDATE BACKUPS

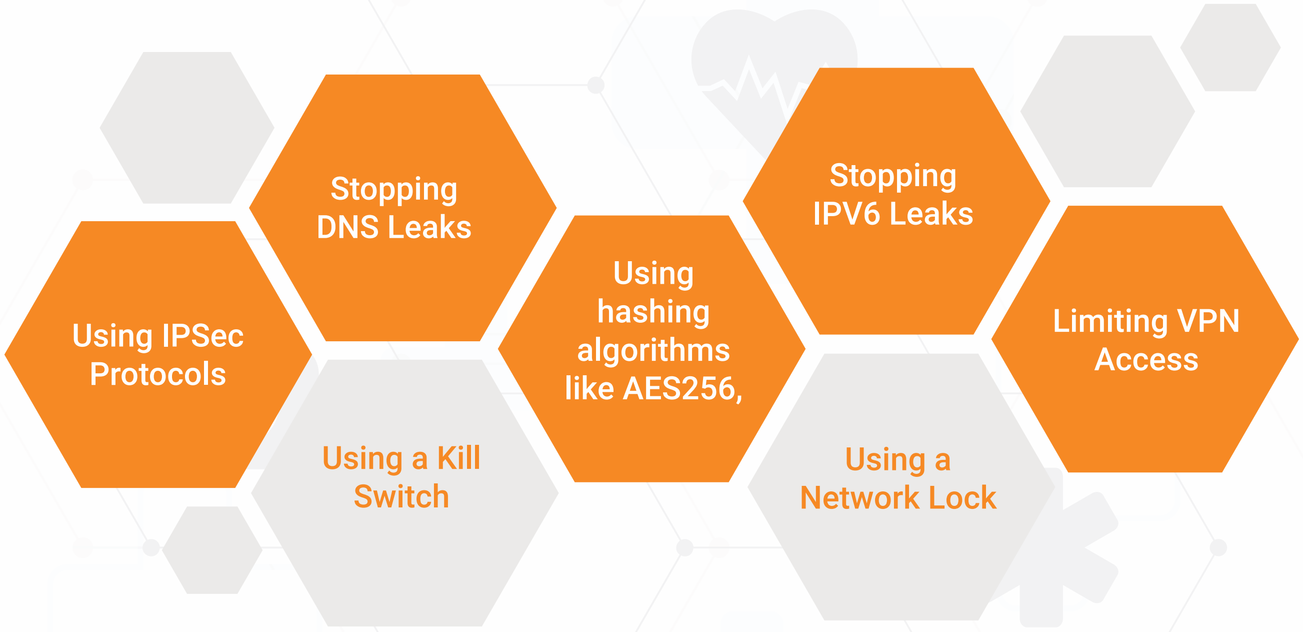
A backup that is stored separately from other backups and is inaccessible from the end-user layer is called a remote backup. Creating an isolated backup helps reduce security breaches, especially ransomware attacks. Ransomware is an attack that quickly encrypts all files on a hard drive and starts attacking other devices connected to a network. Creating local backups is not enough to prevent the system and network from this attack, so isolated backups are the best choice. An organization can quickly recover all its data if it has a remote backup.

A remote backup can be created by moving a backup on remote servers and an isolated network that can be accessed occasionally. Once created, it should be validated from time to time to keep it updated.

IMPROVE YOUR VPN ENCRYPTION

A VPN (Virtual Private Network) helps you establish the private network while using the public networks. You can encrypt your internet connection and hide your online identity using a VPN. VPN encryption is a process by which a VPN hides your data when it enters and passes through its tunnels.

Being a healthcare organization, hiding your network details is essential as much critical data is being sent and received over your network. When using a VPN, you can stop attackers from getting any information regarding your network even if they already monitor it.



Using IPSec Protocols

Stopping DNS Leaks

Using a Kill Switch

Using hashing algorithms like AES256,

Stopping IPV6 Leaks

Using a Network Lock

Limiting VPN Access

REMOTE WIPING & DISABLING MOBILE DEVICES

Remote wiping and disabling is a way to remotely remove or lock the data and user accounts from a mobile device if it is misplaced or stolen. Having remote access to your devices is a significant security feature that helps you control your device remotely.

It is essential that healthcare organizations install remote wiping and disabling on all mobile medical devices to remove their data and accounts if it ever gets stolen or lost. Remote wiping and disabling is a security function that allows you to remotely erase the data on the device or lock the device, even when the device is lost or stolen. You can destroy data stored on your lost or stolen mobile device if you enable the remote wipe feature on your device.

Nowadays, most devices have in-built remote wiping and disabling features that the authorized user can easily enable. But, if a device does not have it, any remote wiping and the disabling tool could easily be installed on the device.

USE EFFECTIVE EDR (ENDPOINT DETECTION & RESPONSE) TOOLS

Attacks can be easily contained with endpoint detection and response (EDR), coordinated visibility, and network segmentation. The Endpoint Detection and Response Tools (EDR) is the technology that alerts the security teams regarding any malicious activity or security threat. They enable fast investigation and containment of attacks at endpoints (an employee's workstation, a cloud system, a server, mobile or IoT device).

Using Effective EDR tools can help you improve the security of your network by aggregating data on endpoints, including process execution, endpoint communication, and user logins. It is vital to use practical EDR tools to detect and respond to any suspicious activities as soon as they are performed.

HERE IS A LIST OF THE BEST EDR TOOLS:

- CROWDSTRIKE
- FIREEYE
- SYMANTEC
- RSA
- CYNET SECURITY
- CYBEREASON
- SYSTEM CENTER CONFIGURATION MANAGER

MOVE TO A VIRTUAL SERVER

Due to the widespread use of the cloud for data storage, the cloud-based deployment category saw the most considerable absolute growth of 158.74 percent. Organizations need to opt for the on-site or off-site servers depending on their requirements or partner with cloud service providers.

A server that shares the hardware and software resources with other operating systems is called a virtual server. You can re-create the functionality of a physical server through a virtual server. Multiple virtual servers can be set on a single physical server. They help in better resource allocation and utilization and allow for hardware independence, mobility/failover, and advanced disaster recovery. By moving to a virtual server, healthcare organizations can control who accesses their data, information, networks, and systems and improve resiliency and uptime.

Moving to a virtual server is essential as it has so many benefits that address the security concerns that a healthcare organization faces. These benefits include getting the ability to prioritize the critical traffic and improving the network agility while reducing the burden from the IT department.

A healthcare organization can move to a virtual server by using any industry-standard hypervisor (virtualization software), such as:

- VMWare
- Microsoft Hyper-V
- SolarWinds Virtualization Manager
- V2 Cloud
- Parallels Desktop
- Oracle VM Virtual Box

ADDRESS FAST HEALTHCARE INTEROPERABILITY RESOURCE STANDARDS

Healthcare organizations should always ensure the Fast Healthcare Interoperability Resource standards are being addressed. Multiple privacy, security, and usability problems must be solved in order to allow convenient access to patient data, all of which are anchored in identity. Strict authentication rules must be in place when users seek access to their data to ensure that the person requesting EHI is who they say they are. Patient matching issues have plagued the healthcare business for years, and they continue to do so in the absence of national patient identification. Those concerns must also be addressed to deliver the right EHI.

API-level security is also essential. Because FHIR APIs are in the public domain, they must be guarded after access is allowed. To address these difficulties, take an identity-centric strategy to data exchange. Adopting multi-factor authentication, which, while not technically mandated by the new ONC and CMS Rules, is strongly recommended by government guidance

USE TWO-FACTOR AUTHENTICATION

Two-factor authentication(2FA), also known as multi-factor authentication (MFA), is used by most companies to validate who accesses their system. It requires users to verify their identity by using only authenticated users' information. Implementing two-factor authentication in a healthcare IT system is essential to comply with HIPAA laws and protect patients', employees', and other organizational data. Furthermore, it helps secure the system by ensuring that only authenticated and verified users access the system at any given time.

The healthcare organization can implement the two-factor authentication either by developing their system or integrating a pre-built tool such as:

Duo Security	Google Authenticator
Last-Pass	One-Login

THE WAY FORWRD

To prevent an increase in the future data breaches and the financial burdens they bring, it is now necessary for healthcare facilities to adopt the use of a third party IT and infrastructure service team. Not your normal MSP, but specialized and skilled services providers that can handle the difficult cloud and IT management chores, enabling companies to focus on their core competency. In a tech landscape that only grows more complex, there are new “as a service” providers popping up daily. And having the right agency can play a key role in business success. Here are a few types to consider:

Managed Communication Services - This type of services partner will deploy and manage a unified communications infrastructure, including messaging software, VoIP (voice over internet protocol), mobile data services, comprises email, and video conferencing. Having the right communication system, hosted or on-premise, can enable you to communicate effectively, especially with remote offices and mobile users. Communications with a single solution that manages your business effectively and economically

Managed Cloud Infrastructure - Managed Cloud infrastructure services transfer your company's operations from a data center to a high-availability cloud environment. They provide the migration, configuration, optimization, security, and ongoing maintenance of your cloud resources and infrastructure; delivered as a service for a fixed monthly fee. Businesses streamline their cloud networking and simplify application interoperability, by using these experts to maintain their cloud infrastructure, application stacks, tools, and databases.

Managed Networks and Infrastructure - There are many different components that makeup “IT infrastructure” managed service offerings. These teams are responsible for designing systems, upgrading existing systems, and deploying unique applications to support your business operations growth. Their focus is on putting the right system in place to ensure durability and uptime. With this type of service, the partner generally takes on the entirety of network tasks. This includes establishing LAN, WAPs, firewall solutions, data backups, reporting and data analytics, and more.

Managed Security Service Providers - This is a catch-all service for remote security infrastructure. It covers everything from BDR solutions to anti-malware options. Organizations that partner with a managed security service provider (MSSP) will receive real-time, validated alerts should a data breach or other security incidents occur. These partners also include defensive measures such as firewalls, virtual private networks, data encryption, intrusion detection systems, authentication protocols, etc.

Managed Support Services - This type of service provides a help desk staffed with engineers or other skilled technical personnel, either 24/7 or an agreed-upon range of times. While some larger corporations have the resources to fulfill this need internally, many SMBs do not have the budget, bandwidth, or expertise, and therefore choose to outsource their support desk to a managed service provider. This allows their IT teams to shift their focus to more important, revenue-generating projects and also provides an iron-clad service level agreement to improve the user experience.

Data Center as a Service - The second type is known as Data Center as a Service (DCaaS), a hosting service in which physical data center infrastructure and facilities are provisioned to clients. They are responsible for data center operators the ability to run efficient data center controls and improve data center infrastructure planning and design. By outsourcing to a service provider, companies can resolve logistical and budgetary problems related to their on-site data centers. They often offer Data Center Infrastructure Management (DCIM) services, that protect the performance and integrity of the core data center components. The right DCIM team keeps everything connected from change management, and capacity planning, to software integration, and data analysis and reporting.

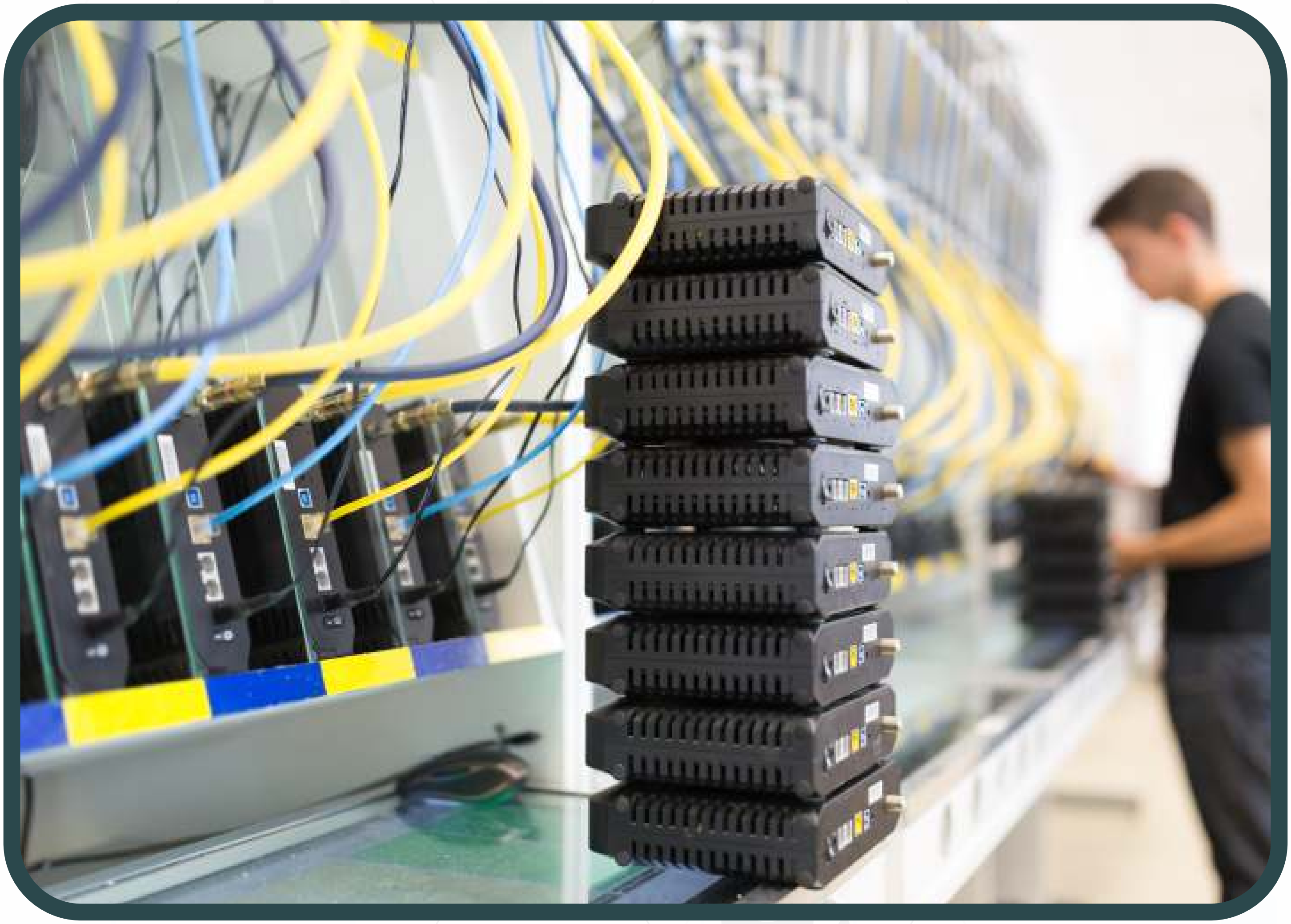
Although healthcare organizations have many options to increase their system and network security and manage the potential threats, it does not meet the level of expertise required to mitigate these threats. Using a professional service is important as you cannot handle all types of threats yourself. You, at some point, will need to seek professional help to tackle the security breaches, so it is better to assign the task of managing the system security to an external agency. This way, you will no longer have to worry about data and network security, and your team will be able to focus on medical-related tasks.

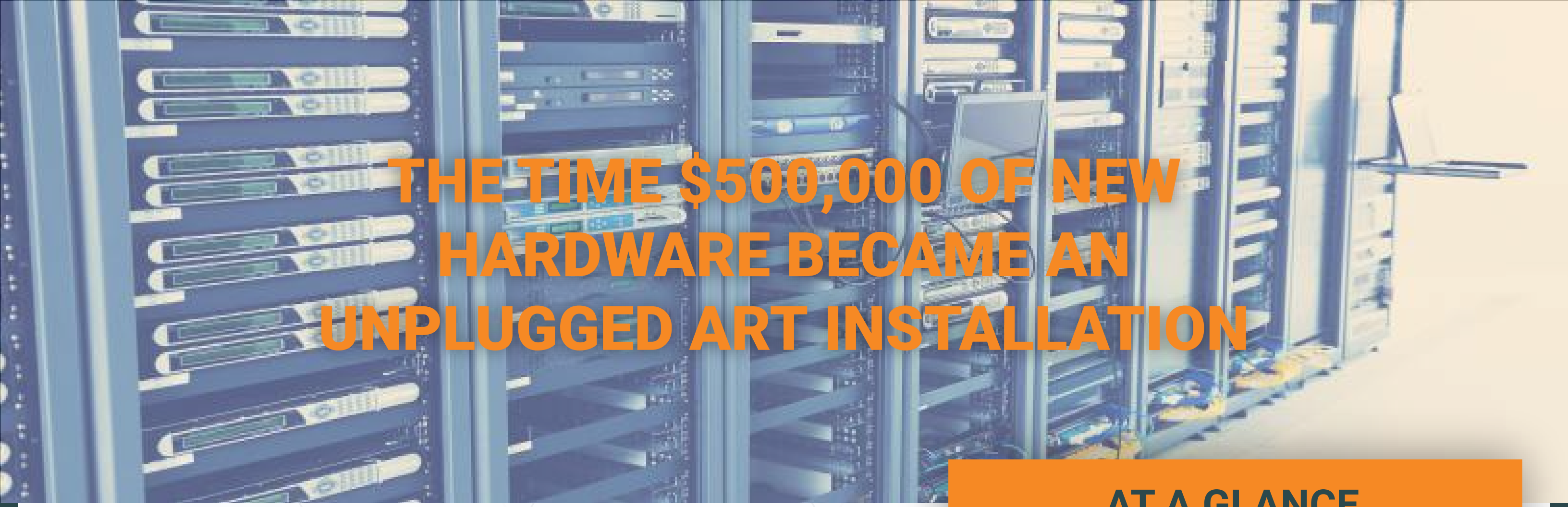
There are so many professional services available to help you protect your data and network, such as Protected Harbor. Protected Harbor provides customized data center infrastructure management and application migration support to businesses looking to scale their technology and bottom line.

Protected Harbor's answer to the current healthcare data breach crisis is to focus on creating advanced structures with high-security levels for our clients before deployment. We also train our clients on best practices, such as usage of new platforms and testing of the infrastructure. To safeguard our customers' operations, we mainly concentrate on six elements throughout the stack, uplink, firewall, switches, hosts, VMs configuration, and storage.

Protected Harbor ensures proper configuration at every point that contributes to improved security and high performance. This is made possible through our infrastructure, which is capable of accommodating sensitive data such as personal health information records. Our professionals have also managed to eliminate multiple challenges that interfere with most database environmental architecture, including the use of wrong relational database management systems and outdated databases, and storage not optimized for database workloads. Other areas where we excel are handling database scalability issues, increasing data volumes, growing database complexities, decentralization management, and poor data security. A well-defined system architecture makes it possible for the company to solve these hurdles and acts as the foundation for improved data quality, information governance, and data management. With the relevant business-scale capabilities, IT and engineering experts develop efficient stacks that handle important database issues such as those mentioned above.

Understanding how a user operates is vital to realizing the kind of system model and securities to integrate. Configuration of devices requiring high availability demands that the involved IT professionals look at the framework from different perspectives, including load balancing layer, platform production space, routing layer, data layer, hosting console, and platform system console.





THE TIME $500,000 OF NEW HARDWARE BECAME AN UNPLUGGED ART INSTALLATION

THE PROBLEM

One of the largest billing companies in the United States had recently invested half a million dollars in new server equipment. Just as they started migrating their biggest customer to the new system, everything crashed, and their business was at risk. Fortunately, Protected Harbors' CEO Richard Luna was on-site at that time for a postmortem with the entire 20-person in-house IT team, regarding another data networking problem that he solved a day or two ago. Panic insinuated throughout the client's conference room as their reputation was on the line and they could see potential financial losses. Moreover, the company's current IT team was unable to diagnose the cause of this and they could not provide swift recovery services, thus losing the confidence of the company.

AT A GLANCE

CONFIGURING HIGH AVAILABILITY FOR ONE OF THE LARGEST MEDICAL BILLING COMPANIES IN THE U.S.

- 680+ Virtual Machines
- 8 Petabytes of storage
- 99.99% Uptime reached
- 50% Increase in application speed
- 1,500% Increase in servers

THE SOLUTION

Richard could not stand by and watch the ship go down. Although they were not an official client, Richard asked the company's CEO if he could step in and help. The future client happily agreed. Richard initiated an emergency deep dive with the IT team, and within an hour developed an action plan. Richard diagnosed that the software configuration was misaligned with hardware. The legacy systems were overloaded without any effective monitoring or regular backups. The servers and storage were simply maxed out. The current design had the database server, remote connection server, and application server all running in a single virtual machine. If the database server needed 90% of the CPU to execute a task, there was not enough bandwidth to keep the other services up and customers crashed. If the remote server needed to be rebooted, the database and application servers would also have to be rebooted, causing the entire system to go down

> *I am glad you all followed the first rule of resolving an IT problem; panic. Nothing produces panic faster than an outage. Now that we are panicked let's focus on what on solving the issue. What is currently good and working?*
>
> **Richard Luna**
> Founder & CEO

THE SITUATION

Richard put together a two-part plan: reconfigure the design and upgrade the hardware. The next day at 4 am, Richard presented the client with 3 hardware options with unique features and prices. After having a meeting with the client, three hours later, it was decided that the company would order the new top of-the-line hardware option, only if Richard and Protected Harbor would help design, deploy and manage the new setup. A new relationship was born.

THE SOLUTIONS

1

Rapid Diagnostic & Repair

Protected Harbor was able to initiate a quick discovery and rapid response based on company standards they have drafted for past clients. By testing and eliminating entire groups of functions, they were able to eliminate possibilities and, narrow down the issues quicker.

2

Software Supported Equipment

One of the core reasons why the equipment malfunctioned was because the equipment installed was not in line with the software ecosystem the client operated on. Hence, it was necessary to identify and install the right equipment to support the client's software, that was both reliable and durable.

3

Hardware High Availability

Moreover, it was necessary to have a fail-safe in place to ensure system uptime even in the event of a failure. The team introduced high availability for the virtual servers by building a failover cluster using state-of-the-art software-defined storage technology. Therefore, adding durability and reliability to the client's infrastructure.

4

Application High Availability

Protected Harbor designed and implemented a high availability configuration at the application layer. In the event of a virtual server malfunction, other virtual servers can continue serving the application. This resulted in a much more secure ecosystem, improved server performance, improved database functions, and reduced dependability.

5

Remote Application Protocol (RAP)

The current setup was a mix of full desktop servers and remote application terminals that allowed customers unrestricted to access the database server. Those customers would eventually make a mistake within the database and the application would break, causing the system to crash. Richard put his new client into a RAP environment, where customers would log into a terminal server to access the app and pass through a restricted gateway to access the database. This essentially made them a RAP app sitting on a pool of 8 terminal servers all linked on multiple database servers.

The new hardware infrastructure increased the reliability, and durability of their services. Their service and reputation grew, allowing the client to go from four to 60 severs in their Data Center since Fall 2018. They now hold 1.8 petabytes of data storage across 680+ virtual machines (VM) with unlimited bandwidth allocation and no metering on egress or ingress. Moreover, their application speed increased 50% and their uptime reached 99.99%. As for the client's largest customer, their business increased by an enormous 500%. They grew from two database servers to 22 database servers, with 49 dedicated VM. They have not experienced a critical outage since Protected Harbor began managing the client's database.

ABOUT PROTECTED HARBOR

Protected Harbor provides customized data center infrastructure management and application migration support to businesses looking to scale their technology and bottom line. With over 15 years of service and a 99.99% uptime record, our team is fully committed to creating, maintaining, and managing the highest quality application operations environment experiences. Your uptime is our focus. Our 90+ Net Promoter Score, and 95% client retention rate back up that claim

Our Protected Data Center is an integrated suite of managed services focused on the uptime of your application at the lowest possible cost, regardless of location, and cloud provider. From infrastructure design to network operations including security, storage, connectivity, remediation, monitoring, and more. Protected Data Center provides end-to-end support to secure deployments of complex enterprise applications to protect your technology infrastructure investments.

Like everyone else, we offer Cybersecurity, Enterprise Networking, Infrastructure Design, Network Configuration, Monitoring, Customized Protected Cloud, Change Management, & Protection & Recovery.

Unlike everyone else, we listen, learn, think, and do not blindly deploy. Focusing on durability and uptime, we design a custom architecture solution integrated with a seamless migration process. The entire time we keep your business up and running with our proprietary application outage avoidance methodology (AOA) providing redundancy and high availability.

www.protecteddatacenter.com

REFERENCES

- **Bitglass survey report**
  https://medcitynews.com/2021/02/report-healthcare-data-breaches-spiked-55-in-2020/
- **Businesswire healthcare data breach report-**
  https://www.businesswire.com/news/home/20210217005003/en/Bitglass-2021-Healthcare-Breach-Report-Over-26-Million-People-Affected-in-Healthcare-Breaches-Last-Year
- **CMS.gov**
  https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index
- **Cybersecurity & Infrastructure Security Agency (CISA)**
  https://www.cisa.gov/uscert/ncas/alerts/aa21-291a
- **Global businesswire (October 2021)**
  https://www.globenewswire.com/news-release/2021/10/28/2322459/0/en/IoMT-Market-worth-USD-187-60-Billion-by-2028-with-29-5-CAGR-Market-Projection-By-Technology-Major-key-players-Growth-Factors-Revenue-CAGR-Regional-Analysis-Industry-Forecast-To-202.html
- **HHS report**
  https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
- **HHS.gov**
  https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html
- **HHS.gov**
  https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/privacy-security-electronic-records.pdf
- **HIMSS**
  https://www.himss.org/resources/interoperability-healthcare
- **Hipaa journal**
  https://www.hipaajournal.com/february-2020-healthcare-data-breach-report/
- **HIPAA Journal**
  https://www.hipaajournal.com/healthcare-data-breach-statistics/
- **Hippa Security standards**
  https://www.cleardata.com/hipaa-security-rule-standards-and-implementation-specifications/
- https://www.hipaajournal.com/healthcare-industry-has-highest-number-of-reported-data-breaches-in-2021/
- **IBM Cost of data breach report 2021**
  https://www.ibm.com/downloads/cas/OJDVQGRY
- **IBM Data breach report 2021**
  https://www.ibm.com/security/data-breach
- **Journal of cybersecurity**
  https://academic.oup.com/cybersecurity/article/2/1/3/2736315
- **Kays Harbor**
  https://kaysharbor.com/blog/healthcare/hipaa-data-breaches-2017
- **PhoenixNAP**
  https://phoenixnap.com/
- **Ponemon Institute report**
  https://www.ponemon.org/news-updates/news-press-releases/
- **Securelink healthcare data report**
  https://www.securelink.com/blog/healthcare-data-new-prize-hackers/
- **Techjury Data breach report**
  https://techjury.net/blog/healthcare-data-breaches-statistics/#gref
- **Verizon Data breach report**
  https://www.verizon.com/business/resources/reports/dbir/
- **Weforum healthcare statistics report**
  https://www.weforum.org/agenda/2021/11/healthcare-cybersecurity/