Healthcare Cybersecurity Playbook

An Evolving Landscape

cloud security alliance®

The permanent and official location for Software Defined Perimeter Working Group is
https://cloudsecurityalliance.org/research/working-groups/software-defined-perimeter/

© 2021 Cloud Security Alliance – All Rights Reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance at https://cloudsecurityalliance.org subject to the following: (a) the draft may be used solely for your personal, informational, non-commercial use; (b) the draft may not be modified or altered in any way; (c) the draft may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the draft as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance.

Acknowledgments

Authors:

Jim Angle
Vince Campitelli
John Di Maria
Eleftherios Skoutaris

Reviewers:

Alex Kaluza
Ashish Vashishtha

CSA Global Staff:

Stephen Lumpe
Claire Lehnert
AnnMarie Ulskey

© Copyright 2021, Cloud Security Alliance. All rights reserved.

Table of Contents

Introduction 5
An Evolving Landscape 5
Healthcare as a Prime Target 6
The Promise of Secure Healthcare 10
Protecting all Patients all the Time 11
Scalability for Today and The Future 12
Time, Money, and Resources 14
Managing the Entire Lifecycle 16
Elevating Your Security Posture 20
Conclusion 21
Training and Education 21

© Copyright 2021, Cloud Security Alliance. All rights reserved.

Introduction

An Evolving Landscape

To understand where healthcare currently is regarding the use of technology, it is helpful to look at how we got where we are. What obstacles there were and how healthcare overcame them? What kind of changes can healthcare expect and who will lead these changes?

During the 1950s, the thought of using computers for automating selected nursing activities and records started us on our journey in the information age. At that time not very much was accomplished moving us along, because computing had not evolved enough. Additionally, the medical community did not see the value and did not have the interest in computerizing healthcare.

In the mid-1960s, vendors started developing hospital administration programs. The late-1960s saw the rise in shared hospital accounting systems, allowing small and medium-size hospitals to utilize these services. Additionally, computer systems for clinical use were attempted but were unsuccessful.

In the 1990s, computers were becoming more powerful and flexible, making them practical as information management tools. Also, networking was introduced at this time, which allowed for the linking of healthcare data from different locations. This, coupled with the growing importance of patient-centered integrated data, shifted the focus to lifelong health records (Hannah, Ball, & Edwards, 2006). Until this time very little work was done on the use of computers in the clinical process. The biggest obstacle for advancing computer use was the reluctance of vendors to document the advantages in terms of economic and patient health benefits (mThink, 2003).

From these beginnings' healthcare has moved at a rapid pace to computerized health records. Today, patient's have their completed medical history in a record that can be retrieved, viewed, and amended from multiple locations and multiple providers. This also brought healthcare into a time of innovation and opportunity focused on clinical care.

This digital transformation has changed healthcare in ways that were not possible just a few years ago. The use of cloud computing and big data analytics, coupled with the move to consumer-centric healthcare, is reshaping healthcare delivery. Healthcare Delivery Organizations (HDO) have access to large quantities of data that can provide tremendous benefit to both the HDO and the patient if collated, analyzed, and properly utilized.

With the use of cloud computing comes the Internet of Things (IoT) and the use of wearable medical devices termed the Internet of Medical Things (IoMT). These innovations have provided large amounts of data bringing with them the promise of improved patient care, better clinical data, improved efficiency, and reduced costs (Armis, 2019).

Not too many years ago, medical devices were stand-alone devices that did not have any network connectivity. Today's medical devices not only have network connectivity but often connect to the cloud. This connection has numerous advantages. First, it allows for remote monitoring of devices. Providers can see how implanted devices are working without the patient having to come

© Copyright 2021, Cloud Security Alliance. All rights reserved.

to the provider's office. In hospitals the nursing staff can monitor patients from a central location eliminating frequent visits to the patient's room.

One aspect of healthcare that has increased significantly during the COVID-19 pandemic is the use of telehealth. Telehealth is used for everything from remote patient monitoring to routine appointments as healthcare delivery transitions toward a patient-centric model. Additionally, with the onset of the COVID-19 virus, HDOs commonly rely on videoconferencing for routine outpatient visits. Telehealth can dramatically bolster efforts to reduce patient exposure to other patients, staff members, and vulnerable populations if utilized effectively. It can also deliver needed care to individuals with mild symptoms in their homes while slowing the spread of a deadly virus.

These advances in technology coupled with cloud computing have brought us to the point where we now have enormous data sets. These data sets can be used with big data analytics to manage population health, predict health trends, and manage pandemics, as shown with the COVID-19 response. This data analysis can lead to patient outcomes.

Healthcare as a Prime Target

By any measure, the US Healthcare Industry is a target rich environment! The industry is supported by over 784,626 organizations comprising thousands of complex and dynamic supply chains. The industry employs one in every 8 US citizens. Annual admissions in the over 6,210 registered hospitals number over 36 million per year. This does not include the post-Covid pandemic surge in telemedicine and telehealth services, creating a new class of patient services, admissions and treatments [1].

The magnitude of expenditures in the United States is manifested by the fact that since 2010, the annual healthcare expenditures in the US have comprised over 17% of gross domestic product (GDP) [2].

Cloud computing - a small pond in a huge lake

Cloud computing is still in its infancy, in an industry that started experimenting with technology in the 1950s. But the pace of adoption is projected to continue to increase at an increasing rate, as illustrated in Chart 1[3].

With this growth, it is projected that for many of the reasons noted throughout this playbook, the risk of cybersecurity attacks will reflect similar if not greater frequency rates than experienced in the existing legacy technology platforms that currently pervade the industry. According to a 2019 Thales Report [4] 70% of healthcare organizations surveyed reported a data breach, with a third reporting a breach within the last year. All organizations surveyed reported collecting, storing, or sharing sensitive information with digital transformation technologies.

[1] https://policyadvice.net/insurance/insights/healthcare-statistics/
[2] IBID
[3] https://www.mordorintelligence.com/industry-reports/global-healthcare-cloud-computing-market-industry
[4] https://cpl.thalesgroup.com/healthcare-data-threat-report

© Copyright 2021, Cloud Security Alliance. All rights reserved.

"Between 2009 and 2019, there have been 3,054 healthcare data breaches involving more than 500 records. Those breaches have resulted in the loss, theft, exposure, or impermissible disclosure of 230,954,151 healthcare records. That equates to more than 69.78% of the population of the United States. In 2019, healthcare data breaches were reported at a rate of 1.4 per day." [5]

According to an article published January 5, 2021, in Health IT Security, Cyberattacks against healthcare entities rose 45 percent since November 2020. At this rate, the sector is accounting for 79 percent of all reported data breaches, according to reports from Check Point and Fortified Health Security.

Check Point's research provided a fresh analysis of the biggest threats currently facing the sector. Shortly after the federal agency alert on the imminent ransomware threat facing healthcare providers, researchers observed a 45 percent increase in attacks—more than double the amount seen in other industries.

Chart 1

The threats include botnets, remote code execution, and DDoS attacks, with ransomware attacks seeing the biggest increase. Check Point stressed that malware is the biggest threat facing healthcare providers.

This information confirms our thesis that the healthcare industry faces significant challenges, somewhat unique to other industries, namely:

Providing adequate healthcare requires collecting huge amounts of sensitive data that pose significantly longer-term risks than other industries. Moreover, the data is inherently more attractive to hackers than other types of data that can be accessed and exploited. As a result, there may be a cascade of negative impacts to successfully attacked organizations such as: significant fines/penalties or legal actions extracted by regulatory agencies such as HHS, FDA in the USA and GDPR in the European Union and the European Economic Area; in addition, there is always the loss of patient and community confidence as well as reputational damage to the organizations implicated.

From a risk perspective, the potential for future damages cannot be fully mitigated. For example, in financial services, credit cards can be canceled and bank accounts closed. In healthcare, private patient data can be re-sold, recycled, and reused in an endless cycle of fraud and abuse! Even worse, the patients may never be aware of the fraud associated with their data! Without improved and more effective interventions, the outcomes are only too predictable and alarming.

As more sensitive healthcare and related personal data move to the cloud, spurred by the growth of individual providers and new entrants into the market, the volume of targets will grow, and the volume of data will grow exponentially.

[5] HIPPA Report https://www.hipaajournal.com/healthcare-data-breach-statistics/

© Copyright 2021, Cloud Security Alliance. All rights reserved.

Patients globally will continue to come to the US to seek the outstanding healthcare services only available in America. This places a compliance burden emanating from the European Union - The General Data Protection Regulation, aka, GDPR. Such activity triggers two regulatory requirements. Under the US HIPAA requirements, the periodic risk assessments must document the existence of these cross-border data flows, and under the EU's GDPR, the data protection requirements necessary to achieve compliance. In addition, with the UK exiting the EU on January 1, 2021, under the Brexit accords, GDPR as it currently exists in the UK will certainly undergo modifications.

Healthcare is also a study in managing supply chain risk. Organizations should not naively assume that they don't have to worry about security because they're moving to the cloud. Providers continue to be responsible under HIPAA for completing and documenting an enterprise risk assessment, including the risk associated with outsourcing to third-parties, especially where the nth? parties of third parties may subsequently be responsible for the operation of selected security and privacy controls. In short, Providers are responsible for validating and vetting their Cloud Service Providers to ensure they are capable of meeting their regulatory requirements such as HIPAA and GDPR. Moreover, healthcare providers that rely upon Cloud Service Providers (CSPs) need to understand that regardless of individual CSP responsibilities, the healthcare provider is accountable for the adverse outcomes resulting from the deficient or non-conforming practices, of the business associate(s) providing the service. Now, more than ever, the security axiom that a strong organization is only as "strong" as its weakest link is a mantra to be embedded in the spirit and practice of all provider due diligence practices.

It has been our observation that organizations adopting cloud services come to realize that with the adoption of every new CSP, they have essentially extended their enterprise into another entity "somewhere in a cloud." One that they have limited control over and even less visibility into their operations, but remain fully accountable for the continuous operation, effective performance, appropriate security, privacy, and all relevant regulatory compliance requirements. While not impossible, success is not a given without insightful planning, continuous vigilance, and mastery of the technology services being delivered throughout the supply chain. These new challenges may pose considerable budgetary and training burdens on organizations trying to balance patient care and the economic stress of operating in a global pandemic.

Addressing the cybersecurity and cloud technology skills gap in healthcare. One of the most prevalent challenges to most healthcare organizations entering 2021 will be mastering the upskilling and new skilling requirements to meet the unique needs of digital transformation and cloud technology platforms, including governance, risk, compliance, security, and privacy.

Current State of Healthcare Cybersecurity

In order to reflect the most current snapshot of cybersecurity status in the United States, recent results of surveys conducted in 2020 are being shared to provide some insights into current trends and challenges for the industry.

One recent market research study [6] which surveyed 2,464 security professionals from 705 healthcare

[6] https://www.prnewswire.com/news-releases/attacks-predicted-to-triple-in-2021-black-book-state-of-the-healthcare-industry-cybersecurity-industry-report-301172525

© Copyright 2021, Cloud Security Alliance. All rights reserved.

organizations, was designed to understand why such organizations were susceptible to healthcare-related data breaches. As illustrated in Figure 1, below, the researchers found [7] :

1. 73% of the health system, hospitals, and physician organizations assessed their infrastructures as unprepared to respond to cyberattacks
2. 96% of IT professionals confirmed the sentiment that data attackers are outpacing the ability of their enterprises to rebuff attackers.
3. Talent shortage for cybersecurity professionals continues unabated. It far exceeds the demand by health systems.

In a related Black Book survey, 291 healthcare human resources executives were surveyed.

They reported that health IT roles can be challenging to fill, often taking 70% longer than other IT jobs.. An additional 66 CISOs of health systems that were also interviewed disclosed their beliefs that many security professionals would be disinclined to seek employment in healthcare organizations.

Figure 1

In summary, the existing gaps in healthcare cybersecurity, combined with the lack of appropriately experienced IT professionals in the health sector, increase the likelihood of healthcare breaches. These cybersecurity risks have only been compounded by the increase in a work-from-home environment, with a large number of healthcare workers required to work from home without the benefit of comprehensive and tailored security guidelines and best practices designed specifically for these new work paradigms.

Healthcare & Cybersecurity – Key Industry considerations (3)

- *It has been predicted that the healthcare industry would suffer 2-3 times more cyberattacks than the average no of attacks for other industries*
- *Ransomware attacks on healthcare organizations are predicted to quadruple between 2017 and 2020, and could grow to 5X by 2021.*
- According to a report in the HIPAA Journal, healthcare email fraud attacks have increased 473% in two years.
- According to a report in Health IT Security, over 24% of US health employees indicated they were not provided cybersecurity awareness training but should have received it.
- More than 93% of healthcare organizations have experienced a data breach over the last 3 years, and 57% acknowledged more than 5 data breaches during the same timeframe.

[7] https://www.herjavecgroup.com/healthcare-cybersecurity-report-2021/

© Copyright 2021, Cloud Security Alliance. All rights reserved.

- It's been alleged that an average healthcare organization's cybersecurity portion of its IT budget can range from (4 - 7) %, compared to approximately 15% in other industries, e.g., financial service.
- IT research firm Gartner predicts that by 2020, more than 25% of cyberattacks in healthcare delivery organizations will involve the Internet of Things (IoT).

The cyber facts defining the healthcare industry are irrefutable! When it comes to cybersecurity, it is an industry under siege. Because of its size, it is an easy target. Due to its culture and an overarching commitment to patient care and health, security and privacy issues are less than organizational imperatives. Hence outcomes are predictable, many attacks are successful, and the successes often have long-lasting effects.

If performed effectively, the adoption of cloud computing may provide healthcare providers with unique opportunities to modernize their care and delivery systems and integrate security and privacy capabilities that would have been unachievable with on-premise solutions. This thesis is borne out in a recent study performed by riskrecon(8), in which it was concluded that ..."We could interpret these results to proclaim that the cloud isn't ready for healthcare applications and should be avoided. Another interpretation, however, might suggest that it's more about institutional readiness for the cloud than the inherent insecurity of the cloud. Either way, these results should encourage all healthcare organizations migrating to the cloud to assess their capabilities for handling the paradigm shift that is cloud security..."

The Promise of Secure Healthcare

Only in the healthcare do we have a paradox in which more data than ever is flowing through physicians' offices and public health departments: however, in the past the value of that data has gone largely untapped because it is unstructured and siloed in systems that don't talk to one another (Kelly, 2019). Today, big data analytics are more important than ever. Big data can be used to help identify COVID-19 outbreaks fast and allow for better responses. Big data can also be used to correlate data on treatments which can aid in ending the pandemic.

As HDOs continue to gain competitive advantages through improved access, quality, and cost, they rely on technology to deliver an advantage. This move started with electronic medical records and the increased reliance on technology to deliver healthcare with connected devices and now has moved to virtual healthcare. The move to virtual healthcare has accelerated in the last year due largely to the COVID-19 pandemic.

The increased use of virtual healthcare coupled with wearable personal health monitoring devices has dramatically increased the attack surface. Add to the mix that commercial nonmedical companies are now involved with Amazon announcing the expansion into nationally available telehealth and Google's purchase of Fitbit. We now have an even larger attack surface. The question now is, with this increase, how do we make good on the promise of access to quality, cost-efficient, and secure healthcare?

The promise of improved practices and standards for patients and providers can be realized using secure and safe technology. To enhance this technology, HDOs are moving more and more of

© Copyright 2021, Cloud Security Alliance. All rights reserved.

it to the cloud. Cloud computing can enhance the performance of HDOs, but due to regulatory requirements, healthcare requires a secure and auditable platform. Cloud computing can link all of the siloed systems allowing data to be collected and analyzed. Cloud computing is helping keep the promise of improved patient outcomes and better provider-patient communications.

Protecting All Patients All the Time

Cloud computing exploded into our environment as a promising technology that would transform the healthcare industry. Cloud computing has many benefits like flexibility, cost and energy savings, resource sharing, and fast deployment (Al-Issa, Ottom & Tamrawi, 2019). Cloud computing also raises many security and privacy concerns. In today's mobile society HDOs require access to medical records at any time from anywhere. Cloud computing facilitates data sharing from patients, medical devices, the Internet of Medical Things (IoMT), and multiple HDOs. This sharing, along with the anytime anywhere access by HDOs and patients, requires an enhanced level of security.

HDOS are responsible for ensuring the privacy and security of healthcare data regardless of where the data resides. Healthcare data is valuable, and HDOs are targets of cyber criminals. This always makes it imperative that HDOs protect all patient information. In addition to the moral obligation to protect patient information, there are also regulatory requirements.

Most countries around the world also have data protection laws that govern the processing of health data. The requirements may be outlined in national law (which apply to personal data in general) and sectoral laws (which apply to a particular field (e.g., health) or specific laws (which applies to a particular situation, such as Covid). Each law has its requirements which may come in addition to another law or as an exception to another law. In addition, due to the discrepancies between the data protection regimes from one country to the other, most countries prohibit the transfer of personal data (including health data) to another country unless certain conditions are met. HDOs must understand the laws governing where their data is collected, processed, and stored; this includes all national and local laws.

Transparency and Assurance

There is a growing realization that the current upward trend in security incidents and poor performance by many organizations is being accompanied by poor levels of public trust. Low confidence in the information communicated in public reporting is probably undermining the motivation for this disclosure. There is a credibility gap that can be narrowed through the use of third-party independent assurance. However, this is not an unqualified solution. Much verification and assurance practice itself has to date been of questionable robustness, reliability, and consistency, and has been framed by assurance models that are inadequate for the broader, qualitative dimensions of performance.

There is a need for a universal framework for the provision of assurance of transparent and ethical reporting and the credibility of the assurance providers themselves. CSA STAR Program offers an approach and tools for addressing these gaps.

© Copyright 2021, Cloud Security Alliance. All rights reserved.

The Security Trust Assurance and Risk (STAR) Program encompasses key principles of transparency, rigorous auditing, and harmonization of standards. Companies that use STAR indicate best practices and validate the security posture of their cloud offerings. The Cloud Control matrix is the baseline sector-specific cloud controls that the STAR program is built upon.

The STAR registry documents the security and privacy controls provided by popular cloud computing offerings. This publicly accessible registry allows cloud customers to assess their security providers to make the best procurement decisions.

To drive business success using the cloud, you must understand the Shared Responsibility Model (Figure 2), and clarity over individual roles and responsibilities is essential. STAR requires organizations to consider roles and responsibilities for both cloud service providers and users.

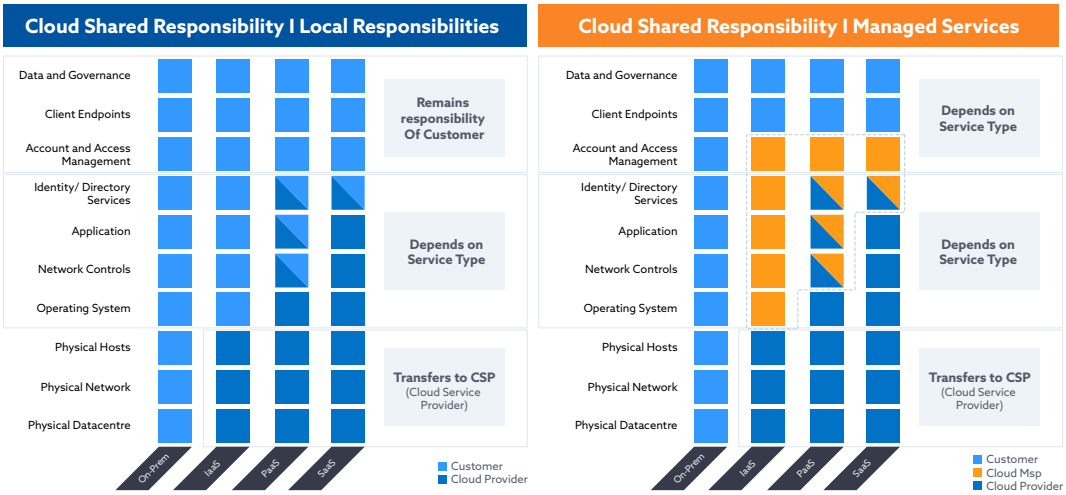

Figure 2

Outages, interruptions, breaches, and disasters are still a risk, even for the cloud. So as a cloud user, you have to identify your risks and implement the associated controls.

Scalability for Today and The Future

It should not be surprising that scale and scalability are two of the watchwords that describe the healthcare industry and cloud computing! They apply to cloud computing in the virtual world that supports the cloud technology processes that allow dynamic expansion or contraction of IT resources. They apply primarily in the physical world to the healthcare industry as measured by the huge number of potential patients/consumers to be served. Over the last year, we have observed how the industry adopted the concept of scalability in the form of cloud computing solutions that supported the unforeseen spike in patient illness and care attributable to the COVID-19 pandemic.

Historically, the size and scope of the US Healthcare Industry have required huge investments in technology resources, processes, and people. These investments have resulted in ongoing capital costs, legacy technology platforms, and immutable infrastructure and real estate commitments. Today, constant and sometimes unanticipated changes in both supply and demand - witness the

© Copyright 2021, Cloud Security Alliance. All rights reserved.

impact over the last two years of the COVID 19 pandemic – are significant drivers of the use of IT. Current trends point to continued growth in demand for healthcare, largely attributable to population aging and growth combined with increasing interest and wellness by consumers. There are four major trends that have been associated with growth rate trends of 11 – 17% thru 2025 [8] :

- Escalation of consumerism. This has had the effect of re-focusing the provider market from volume-based services to value-based. The value model rewards providers based on care cost-effectiveness and clinical case outcomes. These changes warrant rapid innovation enabled by the variable on-demand IT resources achievable with cloud computing. Cloud computing enables consumers to identify and use best-of-breed health services from a large array of providers.
- *Impact of healthcare regulation and restructuring of financial risk*. Healthcare reform and regulation have and will continue to change the healthcare landscape. Regulation influences the market structure and this will continue to drive consolidation both vertically and horizontally. The resulting growth in organizational size and scope, foster larger investments in innovative services and products that appeal to a broad base of consumer/patients. Further impacts of consolidation spawn the inception of new technology platforms and services that create new products and services enabled by cloud computing, such as Big Data analytics and artificial intelligence.Impacted operational processes: In this use case, information procr data security and privacy protection. A unified security management mechanism needs to be considered.
- *Influence of digitalization*. IT, specifically cloud computing, is the enabler that empowers consumers to take greater ownership of their healthcare and provides them access to more choices with less constraints. The healthcare industry is moving towards an information-centric delivery model that fosters cooperation, collaboration, and information sharing. Cloud computing provides the virtual infrastructure that allows hospitals, medical practices, insurance companies, research facilities, and other players in the healthcare\ ecosystem to leverage the same computing resources.
- *Focus on preventative healthcare*. Today consumers upon mobile applications, the Internet of Things (IoT), and wearable technologies - all cloud enabled-to monitor their health, communicate with their providers and receive treatment. Healthcare is evolving from a "fix-me system " to a "promote well-being" system, largely attributable to technological innovation.*Need for medical practice and healthcare delivery transformation*. The promise of today's cloud-based technologies, combined with many technological innovations built on data analytics, artificial intelligence, global collaboration, and ubiquitous access, will hasten industry transformation. The ability currently exists to provide time and location independent, collaborative, consistent, and real-time cognitive patient support and service. These are the types of capabilities that will help to achieve the necessary transformations for healthcare in the future.

To obtain the many benefits provided by the adoption of cloud computing and leverage them across the healthcare landscape, several deliberate steps consuming organizations should follow to cost-effectively and efficiently utilize the many services available through cloud service providers. These steps must take into consideration the dynamics of the consuming organization and both the scale and scope of the services they will be required to provide.

Guidance for Leveraging Cloud Computing for Healthcare [9] :

[8] Cloud Standards Customer Council Impact of Cloud computing on Healthcare, version 2 (2017)

[9] IBID

© Copyright 2021, Cloud Security Alliance. All rights reserved.

1. Build a business case for cloud computing.
2. Identify and prioritize specific cloud based healthcare solutions.
3. Determine the appropriate cloud deployment and service model.
4. Perform a HIPAA compliant. Enterprise risk assessment for all cloud services and cloud service providers.
5. Ensure all security and privacy requirements are addressed.
6. Document the integration and interoperability points with existing enterprise systems. (this should include all other impacted applications/services in the overall supply chain.)
7. Negotiate cloud service agreements and monitoring tools for all SLA's and KPI's.
8. Develop a responsibility matrix/model for monitoring/managing all cloud services and all cloud service providers.
9. Develop and monitor a risk dashboard for the entire portfolio of cloud services and cloud service providers. *(Note this should be periodically reconciled to a separate inventory of all cloud services and cloud service providers.)*
10. Maintain a report with relevant distribution on all high risk open issues.
11. Documenting the corrective action plan(s) and status.

Time, Money and Resources

In a recent survey taken at a CynergisTek's CAPP [10] conference, 54% of Healthcare professionals noted resources (Money, people, tools) as being their biggest barrier in meeting their organizations security and privacy needs. Using the NIST Cybersecurity Framework as a measuring stick, it was found that 79% of healthcare facilities assessed scored less than a "C" in terms of compliance.

More times than not, the root cause is too much complexity. Complexity taxes the systems as well as resources. The more complex systems become, the less secure they become, even though security technologies improve. There are many reasons for this, but it can all be traced back to the problem of complexity. Why? Because we give a lot of attention to technology, and we have increased silos of a plethora of regulations and standards. Therefore, we become fragmented and too complex.

Complexed systems:

- have more independent processes, and that creates more security risks.
- have more interfaces and interactions and create more security risks.
- are harder to monitor and, therefore, are more likely to have untested, unaudited portions.
- are harder to develop and implement securely.
- are harder for employees and stakeholders to understand and be trained on.

To respond to these growing business concerns, the Cloud Security Alliance (CSA) created the Cloud Control Matrix (CCM). Developed in conjunction with an international industry working group, it specifies common controls relevant for cloud security and is the foundation on which CSA STAR is built. The CCM maps to over 35 different standards and regulations. This facilitates decreasing the implementation of a security program significantly.

[10] https://docs.google.com/document/d/1_2RqUOgWB3WWa8bto_dpeyJcyCXy_ZyV58p_lmCg0OQ/edit?ts=608f0a23#

© Copyright 2021, Cloud Security Alliance. All rights reserved.

We should be spending 80% of our time planning and 20% of our time implementing, but in reality, most organizations spend 20% of their time planning, 20% of their time implementing, and 60% of their time firefighting, which then ends up lasting the life of the system or to our retirement whichever comes sooner.

Let's break these down and how they affect a project.

The time constraint refers to the amount of time available to complete a project.
The cost (money) constraint refers to the budgeted amount available for the project.

Resources relate to the amount of people, processes and technology required to ensure a good quality and effective system.

But we must also throw scope into the mix. The size of the project's scope will have a big effect on the time cost and resources. An increased scope typically means increased time and increased cost, a tight time constraint could mean increased costs and reduced scope, and a tight budget could mean increased time and reduced scope.

In the end, how secure your organization is, is a direct result of the complexity. Integrating systems reduces cost and increases security.

An Integrated Security System enables organizations to align their processes and procedures into one complete framework that can help to deliver their objectives effectively and efficiently.

For these systems to be an integral part of the company's overall system, there have to be linkages to seamless the boundaries between processes.

Do things differently...
Experience teaches that the more successful businesses embed best practice holistically across the entire organization, not just in one specific area. Products and services today must meet a diverse spectrum of certification and compliance requirements. Developing a consistent framework of repeatable processes and procedures allows the organization to comply, grow, and protect the operation.

Instituting a company-wide strategy breaks down long-established silos separating departments and divisions and, for many organizations, can represent a significant change to corporate culture.

An integrated security system integrates all components of a business into one coherent system to enable the achievement of its purpose and mission and maintain the system with minimal cost, time, and resources while reducing risk and becoming more resilient.

© Copyright 2021, Cloud Security Alliance. All rights reserved.

Managing the Entire Lifecycle

Any discussion about cloud security should start with the data lifecycle. When defining the required security controls for cloud implementation, remember it is all about the data. Computers, including cloud computing, create, store, process, and use data. The value is in the data, and that is what we are trying to protect. To protect data, we must know what data we have and where it is stored. The best way to ensure you have looked at all security aspects is to look at it through the data lifecycle. Lifecycle management of data is critical because, over time, the value of data may decline; however, the cost of storing the data and the risk of exposing the data does not. When looking at the data lifecycle, it is useful to use the terms defined in cloud computing. The data lifecycle is:

- Create -data is generated, acquired or modified
- Store - data is committed to a storage repository.
- Use, when data is processed, viewed or used in any other sort of activity.
- Shared, data or information is made accessible to others.
- Archived data is placed in long term storage.
- Destroy, when data is no longer required it is physically destroyed.

Create:

Healthcare Delivery Organizations (HDO) create and collect data for numerous reasons such as financial, supply chain, human resources, and patient data. The very first step is to identify what type of data is being created. Is this sensitive data such as Protected Health Information (PHI), Personally Identifiable Information (PII), or Payment Card Industry (PCI) data? Following this the key security factors in this stage are:

How is the data created, collected, or modified? Is it created by an external source, i.e., a new patient or employee entering the initial data? Is it created by compiling data for other data sources? Is it collected by keyboard entry, mobile application, or combining data? The HDO must know the sources of all data.

What will the data be used for? This is critically important for HDOs as both the PII and PHI laws require the HDO to be able to inform the data subject what the data collected will be used for.

Who can create or collect the data? Identifying who can create or collect data is particularly important when the data contains PHI. "Who" reflects on the integrity of the data.

What is the data classification and categorization? The classification of data relates to the confidentiality requirements for the type of data. For example, it could be for internal use only, business-sensitive, or PHI sensitive. Categorization defined in Federal Information Processing Standards (FIPS) 199 establishes three potential levels of impact (low, moderate, and high) relevant to securing information and information systems for each of three stated security objectives (confidentiality, integrity, and availability) (Stine, Kissel, Barker, Fahlsing, and Gulick 2008).

© Copyright 2021, Cloud Security Alliance. All rights reserved.

How secure are each of the tools leveraged to create data? Does the vendor have implemented secure development practices including application code scanning, appropriate access control to code and protect their intellectual property?

Understanding the source of the data will enable the organization to build a solid secure foundation.

Store:

The HDO storage management policy should enable the HDO to effectively manage their storage resources while complying with all laws and regulations. Before the HDO can determine storage requirements, they must understand how much and what type of data they are storing. The following questions can help start the conversation regarding storage:

Where will the data be stored? Will it be in the cloud, in an enterprise data center, locally stored, or on removable media. Each of these has different requirements, and the HDO should consider the implications for each type of storage.

Who has access to the data in storage? It is key to understand the access privileges of those responsible for managing the data storage infrastructure.

For data in the cloud, where is it stored? It is essential to know where the data is stored, both primary and backup data. Is the data stored offshore? The regulatory requirements may be different depending on the storage locations.

How long will the data be required? The retention requirement may drive the storage method.

Is there a requirement for encrypting data at rest? Due to the sensitivity of the data, there may be a regulatory or business requirement for encryption.

Knowing what type of data is being stored, where it is stored, who has access to it in storage, its state in storage, and how long it is required will enable the HDO to implement the correct security controls.

Use:

As data collection continues to increase in speed and scale, the analytic techniques used to process these datasets become more sophisticated, and the use of data becomes more varied. There is a huge potential for big data for health research; however, proper care must be taken to prevent the loss or misuse of the data. Data security in healthcare is about both enabling positive outcomes and stopping negative consequences. Additionally, transparency presents a complex challenge for data security in healthcare. HDOs need to be transparent in how they use data while maintaining security.

Understanding the data and how to use it is critical. The HDO must know the answers to the following:

Who is the user of the data? The data user may not be the owner of the data.

© Copyright 2021, Cloud Security Alliance. All rights reserved.

Where will the data be used?

What is the purpose of the data, and how will it be used?

Is that use appropriate based on data type and regulatory requirements?

How will the data be used in the future?

Gaining a complete understanding of the data and users will help the HDO ensure the right controls are implemented, and they efficiently and effectively protect the data. The controls must include a robust Identity and Access Management (IAM) program. In cloud computing, the old network perimeter is no longer effective, and access becomes the new perimeter.

Share:

For years HDOs built data repositories that were stovepipes where data was confined and isolated. The use of these stovepipe systems led to building systems where data was duplicated rather than shared. Good data security can provide the processes required to share data effectively. To that end, the HDO must answer the following questions:

Who will the data be shared with? For example, an insurance company, billing resources, hospital/ treatment staff?

For what purpose will the data be shared? Do those genuinely have a valid need to know?

Is that use appropriate based on data type and regulatory requirements?

Will it leave the HDO's cloud infrastructure at all? Can the data be adequately protected when used/ stored by these additional providers?

Two technologies that can help HDOs securely share data are a Cloud Access Security Broker (CASB) and Rights Management Service (RMS). The CASB is a policy enforcement center that consolidates multiple security policies and applies them to all HDO instances in the cloud. The CASB allows the HDO to take a granular approach to data protection and policy enforcement. The RMS enables HDOs to augment their data protection strategy by protecting information through persistent usage policies that remain with the information, no matter where it is stored. HDOs can define who can open, modify, print, forward, or take other actions with the information. HDOs can create custom usage policy templates that can be applied directly to the information.

Archive:

Laws and regulations such as the Health Insurance Portability and Accountability Act (HIPAA) demonstrate the need for effective plans for managing the endless array of data that HDOs are creating, processing, and storing. HDOs must implement information security policies not only to minimize liabilities but to improve operations and reduce cost. Data the HDO must maintain but is no longer in active use can and should be archived. It is critical that the HDO fully understands whether

© Copyright 2021, Cloud Security Alliance. All rights reserved.

your data requires long-term data storage, which can have considerable financial and technical hurdles. Archiving data can reduce the cost of storage, long-term storage is cheaper than short term. The HDO must know:

What are the data retention requirements for the various data types within the HDO's control globally?

Does each partner who stores ePHI as part of their service have the means to meet any data archiving requirements?

Are data in an active litigation hold maintained until the conclusion of the hold? (Crosbie, 2020)

Destruction:

The HDO must not forget that data destruction, including asset disposal, is the critical last phase of any data lifecycle. As sensitive, regulated data is leveraged and stored across many locations, the HDO must have clear concise policies and procedures for destruction of outdated restricted data as well as the media on which it is stored if unencrypted. To that end, it is critical that the following questions are answered by the HDO:

Who is responsible for data destruction?

What assurance do the partners provide that data is securely destroyed per agreed upon guidelines?

What are the destruction controls to ensure data is rendered unreadable?

Who is responsible for asset disposal, another aspect of asset disposal?

When an asset is no longer required, is the data on the asset adequately destroyed?

Has the physical storage capability been removed, and the data destroyed?

Does the data destruction policy identify the procedure to ensure all sensitive data is destroyed?

Data destruction for a single entity in a multi-tenant cloud environment is difficult as the media cannot be destroyed for just one entity; it is an all or nothing situation. There are two effective ways to ensure the data is destroyed. First, if the data is encrypted, the keys are destroyed when the data is no longer required. While the data is still physically there, it can never be used (Gillian 2019). One note about this method is that the HDO must ensure that each tenant has different keys for encryption through contractual obligations. Second, the data can be overwritten multiple times until the data is no longer retrievable.

© Copyright 2021, Cloud Security Alliance. All rights reserved.

Elevating Your Security Posture

With the number of security breaches in the news growing exponentially, you need to take action before the next headline is about your organization. But, elevating your security posture can be overwhelming to decide where to begin. Elevating to a strong security posture takes time and continual improvement, however, there are some simple key actions you can take that will facilitate long-term security success.

Create a culture of security awareness, getting leadership buy-in and involve the entire staff to get them on board.

One of the biggest challenges for security professionals is proving the value of investing in security to their leadership or their management. While many leaders may traditionally view security as a roadblock to their organization's productivity, it is imperative to help them recognize the benefits security has.

As many of the breaches today are caused by employee error, an educated staff is one of the most critical parts to a strong security posture. Make sure you implement a holistic training platform that covers all employees. How in depth you go should be dictated by risk and employee roles and responsibilities.

Establish regular security internal audits. Internal Audit is a necessity when it comes to identifying vulnerabilities in a security environment. It's critical to assure you have full visibility into your business processes and associated security posture.

In healthcare, software is used extensively from patient registration to controlling and monitoring active medical devices that transmit body function information as well as dispensing medications. The potential for supply chain attacks and breaches have always been a problem but recent examples like SolarWinds, remind us that attackers can leverage third-party code to directly compromise agency systems. According to a most recent report from sonatype [11], Open Source Software supply chain attacks are up more than 400%, pointing to an increasingly attractive avenue of attack.

The annual Bitglass "Healthcare Breach Report [12] " who analyzes data posted to the "Wall of Shame" breach reporting and public accountability website run by the U.S. Department of Health and Human Services showed that the total count of US healthcare breaches rose from 386 in 2019 to 599 in 2020, an increase of 55.1%. 67.3% of these breaches were caused by hacking and IT incidents. Having a good information security management system in place that covers the critical People, Process and Technology is paramount to surviving the breach. This includes having a good handle on the third-party cloud software (SaaS) and infrastructure companies (IaaS) service providers.

---

[11] https://www.sonatype.com/campaign/wp-2020-state-of-the-software-supply-chain-report

[12] https://www.bitglass.com/press-releases/2021-healthcare-breach-report#:~:text=Bitglass%20News-,Bitglass%202021%20Healthcare%20Breach%20Report%3A%20Over%2026%20Million%20People,in%20Healthcare%20Breaches%20Last%20Year&text=Each%20year%2C%20Bitglass%20analyzes%20data,protected%20health%20information%20(PHI).

© Copyright 2021, Cloud Security Alliance. All rights reserved.

Demanding transparency of evidence of the level of security and effectiveness of your cloud provider is an essential step in mitigating risk as well as understanding your organization›s role and responsibility; as described in the Transparency and Assurance section of this paper, goes a long way in proving due diligence and "standard of care". CSA's Consensus Assessment Initiative Questionnaire (CAIQ) and Cloud Control Matrix (CCM) are excellent tools to start with for very good documented reasons.

Conclusion

Digital transformation and the cloud has changed healthcare in ways that were not possible just a few years ago. The use of cloud computing and big data analytics, coupled with the move to consumer-centric healthcare, is reshaping healthcare delivery. Healthcare facilities have access to a tremendous amount of data that can benefit both the patient and healthcare facilities if used properly. With the innovations of IoT and MedIoT the promise has always been improved patient care. But with this comes responsibility to protect that data and the patients it belongs to.

With 79% of healthcare facilities assessed scoring less than a "C" in terms of compliance, and the U.S. Department of Health and Human Services showing that the total count of US healthcare breaches rose from 386 in 2019 to 599 in 2020, (an increase of 55.1%) there is a definite call to action..... Create a culture of security awareness, getting leadership buy-in and involve the entire staff to get them on board.

Industry and patients are demanding more transparency of evidence of the level of security and effectiveness of your cloud provider as well as your internal organization. In order to mitigate risk as well as understand your organization's role and responsibility; as described in the Transparency and Assurance section of this paper. This along with increased training on security, will go a long way in proving due diligence and "standard of care"; two subjects that will likely come up in the unfortunate event that you are summoned to court. CSA's Consensus Assessment Initiative Questionnaire (CAIQ) and Cloud Control Matrix (CCM) are excellent tools to start with in helping you avoid that "Wall of Shame".

Training and Education

If you are new to cloud computing and even newer to CSA and cloud security, we recommend starting by reviewing the table below of recommended reading materials as well as training and educational opportunities, including CSA certifications.

These documents can be an immense help in identifying the individuals in your organization who can upskill their capabilities and extend their capacity to fill in the knowledge gaps created by the multitude of cloud platforms being utilized and consumed by healthcare providers all over the world.

© Copyright 2021, Cloud Security Alliance. All rights reserved.

Recommended Reading Materials

Below is a guide of reading materials that will help you understand the fundamentals of cloud computing and best practices in creating effective security, privacy and compliance programs.

Reading Materials	Value to the Reader
CSA Security Guidance for Cloud Computing	This paper outlines how security changes in cloud computing and best practices all organizations should follow regardless of which vendor they are using.
Guideline on Effectively Managing Security Service in the Cloud	This provides guidelines for cloud users to better select security qualified cloud service providers. These guidelines are based off of the controls outlined in the Cloud Controls Matrix (CCM).
Telehealth Data in the Cloud	Addresses the privacy and security concerns related to processing, storing, and transmitting patient data in the cloud for telehealth solutions.
Healthcare Big Data in the Cloud	Examines big data and some use cases for big data in healthcare, the impact of big data on healthcare, regulatory requirements for Protected Health Information (PHI) in the cloud, and securing PHI in the cloud.
Managing the Risk for Medical Devices Connected to the Cloud	Presents the concept of managing medical devices based on their proximity to the patient and introduces practices to secure the use of cloud computing for medical devices.
OWASP Secure Medical Devices Deployment Standard	This guide is intended to serve as a comprehensive guide to the secure deployment of medical devices within a healthcare facility.

If you're interested in staying up to date on research CSA creates for the healthcare industry, and/or participating in the creation of future publications you can **visit the CSA Health Information Management Working Group.** This group helps the entire healthcare industry by accelerating solutions to security challenges specific to healthcare. For example, one of our members was able to solve IoT categorization challenges through their participation in this working group.

© Copyright 2021, Cloud Security Alliance. All rights reserved.

Cloud security training we recommend for the healthcare industry.

The whole premise of the training is to train and educate healthcare professionals in the cloud.

More important than earning a certificate, is having robust training for the community working with healthcare organizations. For cybersecurity professionals who are new to the cloud, the Certificate of Cloud Security Knowledge (CCSK) is a good place to start as it will give them a vendor-neutral understanding of cloud computing and security best practices. Once a baseline of knowledge is established, the Certificate of Cloud Auditing Knowledge (CCAK) in particular should be helpful for the core security people in healthcare.

Health Information Management WG: You can see the latest research created by this group or join as a volunteer here.

© Copyright 2021, Cloud Security Alliance. All rights reserved.

References

Al-Issa, Y, Ottom, M, Tamrawi, A, 2019. *eHealth Cloud Security Challenges: A Survey*, Journal of Healthcare Engineering, Volume 2019, Article ID 7516035, https://doi.org/10.1155/2019/7516035

Armis (2019), Medical and IoT Device Security for Healthcare, Retrieved from https://www.armis.com/resources/iot-security-white-papers/medical-iot-device-security-for-healthcare/

Crosbie, Devon, 2020. *Why Data Destruction is Essential to Information Governance*, Complete Discovery Source, Retrieved from https://cdslegal.com/insights/why-data-destruction-is-essential-to-information-governance/

Gillin, Paul, 2019. *Data Destruction in the Cloud: It's Complicated*, Retrieved from https://www.ironmountain.com/blogs/2019/data-destruction-in-the-cloud-its-complicated

Hannah K.J., Ball M.J., Edwards M.J. (2006) History of Healthcare Computing. In: Introduction to Nursing Informatics. Health Informatics (formerly Computers in Health Care). Springer, New York, NY. https://doi.org/10.1007/978-0-387-32189-9_3

mThink, 2003. *Health Care Technology: A History of Clinical Care Innovation* Retrieved from https://mthink.com/health-care-technology-history-clinical-care-innovation/

Stine, Kevin, Kissel, Rich, Barker, William C., Fahlsing, Jim, and Gulick, Jessica, 2008. *Special Publication 800-60 Volume I Revision 1: Guide for Mapping Types of Information and Information System to Security Categories*, National Institute of Standards and Technology, Gaithersburg, MD. Retrieved from Https://csrc.nist.gov/publications/detail/sp/800-60/vol-1-rev-1/final

© Copyright 2021, Cloud Security Alliance. All rights reserved.