Business White Paper

Defense in Depth:
A Pragmatic Approach to Securing PHI in the Cloud

ClearDATA
SECURE • HEALTHCARE • CLOUD

Defense in Depth:
A Pragmatic Approach to Securing PHI in the Cloud

Table of Contents

Page 2
Introduction

Page 2
Not Too Strict

Page 3
Training the Trainers

Page 4
An Inventory of Data

Page 5
BYOD & IoT

Page 6
Share and Share Alike

Page 7
Don't Fail to Plan

Page 8
Risk Assessment

Page 9
Continue Learning: Safest Place for Healthcare is in the Cloud

A savvy executive at a Malaysian tech conference once quipped: "Lunch is not a food!" He was drawing an analogy to the domain of network security. His point? Lunch is an event at which any number of food types can be enjoyed. The same is true for security: there is no single product or policy that encompasses the discipline; rather, organizations must assemble a combination of technologies, procedures and qualified personnel to get the job done.

The irony of that last expression is that, within the realm of security, the job is never done, and never will be. Security is an ongoing process, and one that involves constantly shifting sands. This is especially true in the field of information technology. Every layer of the tech stack in IT is changing, and the pace has actually accelerated in recent years. Form factors like the iPad, architectural disruptions like the Cloud, app-centric issues on the front lines – all of these combine to up the ante on a regular basis.

Consequently, responsible security professionals apply a holistic methodology for engendering a culture of awareness. In doing so, they provide a wireframe for success. They realize that effective security programs will always be a team effort, and so they work to ensure buy-in from throughout the organization. This process involves a balance of training, encouragement, management and monitoring. And the security team must also remain open to new ideas and novel approaches. Achieving security is like hitting a constantly moving target, day after day.

Not Too Strict

One of the most common pitfalls in mapping out a security framework – whether cloud computing is involved or not – is the tendency to tighten controls too much. In doing so, companies can often, perhaps unwittingly, invite workarounds that result in security gaps. It's human nature to be annoyed by constraints, especially when they're viewed as excessive. Thus, when controls are tightened too much, people will chafe at those rules and ultimately find ways around them.

The best way to determine if rules are perceived as being overwrought is to maintain a dialogue with personnel, from the front lines of the business, all the way through the management chain, and even including key partners. By keeping the lines of communication open, the security team can stay on top of the situation and will likely be alerted to any policy or procedure that is viewed as onerous. At the same time, ideas will bubble to the surface for ways to improve important business processes.

The best security experts realize that business process owners are the people who understand why procedures are designed a certain way. They have the domain expertise necessary to explain the who, what, where, why, when and how. They're often the first to know when something is out of line, and usually have developed some means for either fixing it, or circumventing the constraint. This is invaluable information for a security team to glean. Within virtually any organization, you can rest assured that there are many such scenarios playing out every single day.

Many of these control points are being identified as healthcare organizations identify use cases for cloud computing. With software vendors large and small moving to subscription-based offerings, business process owners are realizing just how many points of exposure exist. This is especially true with respect to mobile computing and the Internet of Things, which we'll address later in this article.

Training the Trainers

Almost without exception, the single most powerful tool in the security expert's bag of tricks is education. An old expression notes that adults often don't need to be taught, so much as reminded. That's why regular training programs can play such a critical role. The key is to train the trainers: make sure that the professionals responsible for these programs are using current materials that are relevant for the organization.

One of the weakest links in security profiles is often the end user who falls for a phishing scam. Anyone who spends time interacting with email knows that phishing tactics get more sophisticated every day. Some of the more proficient hackers have managed to mimic the design, layout and content of genuine corporate emails from

major vendors like Verizon, AT&T and other well known brands. Reminding employees and partners to watch out for these scams can help prevent a breach.

The threat of such breaches becomes more apparent with each major incident. In a recent article on *HealthDataManagement.com*, author Greg Slabodkin quoted FBI deputy assistant director Donald Good, who characterizes the healthcare sector as a Tier 1 highly targeted industry. The main reason is because healthcare information systems possess so much critical, personal healthcare information (PHI). Simply put, these systems can be treasure trovers for hackers. Including such assessments in corporate training programs can help employees and partners appreciate the magnitude of the threat.

In another article on *HealthDataManagement.com*, author Joseph Goedert paints a stark picture about why any breach can quickly snowball into a very serious situation. Goedert cites Aaron Hayden, an "ethical hacker" with *CliftonLarsonAllen,* a large certified public accounting firm which claims a 100% success rate at hacking any non-financial organization. This one excerpt from Goedert's article should be sufficient for grabbing the attention of any healthcare industry executive:

"Once in control of one computer, a hacker can assume the identity of the person being attacked. If the person is an administrator, Hayden can install software to read the database password on the computer, as well as passwords from other computers on the network. Once in a network, a hacker can establish persistence - a home - and inject code into startup processes to stay in the network. One university, Hayden said, had 8,000 routable addresses that he could see."

An Inventory of Data

Alongside an ongoing training program, one of the most important components of a comprehensive security portfolio is a data inventory. Security consultants are no strangers to senior executives at healthcare organizations expressing great confidence in the integrity of their systems, only to discover any number of glaring holes. Doing an inventory of PHI is therefore an essential starting point for companies looking to bolster their security programs.

This subject was a key component of a recent webcast with Chris Bowen, founder and chief privacy and security officer with ClearDATA. During the presentation, Bowen outlined key benefits and components of a data inventory, with special consideration for PHI. He noted:

- An inventory allows for a complete account of every element of sensitive data that an organization holds
- Both paper and electronic records should be included
- The inventory will help determine how an organization collects, uses, stores, shares and disposes of its sensitive data—its life cycle
- The inventory also reveals the risks where a breach may occur, so organizations can be strategic in their planning to protect PHI and develop the best plan for a response, based on real information
- On a security level, a PHI inventory means knowing where the systems, servers, and applications that capture and use PHI are and who their business owners and users are
- These owners should understand the regulatory requirements and define the risk of exposure of the PHI, while communicating these risks to the IT and security staff
- Make sure to include the mobile landscape in this inventory
- Disposal of PHI is a critical stage in the lifecycle; any data that is not required to be kept by regulatory mandate should be considered for deletion.

BYOD & IoT

One of the most significant and challenging aspects of security in the cloud-enabled world is the preponderance of new devices that are permeating organizations large and small, usually via programs labeled BYOD, for Bring Your Own Device. These include smart phones, iPads and tablets, but that's just the beginning. Staying on top of all the latest smart phones is a challenge in and of itself. Apple and Samsung are obvious players in this space, but there are many other providers to track.

The larger threat arguably comes from connected devices, sometimes referred to in the context of the Internet of Things. (IoT) In another article on HealthDataManagement.com, author Greg Slabodkin quotes Suzanne Schwartz, director of emergency preparedness/operations and medical countermeasures for the FDA's Center for Devices and Radiological Health. Schwartz noted that networked medical devices "introduce new risks related to potential cybersecurity threats" including the introduction of malware into medical equipment and unauthorized access to configuration settings on devices and hospital networks.

Slabodkin notes that most "medical device manufacturers provide Manufacturer Disclosure Statement for Medical Device Security forms to assist providers in assessing the vulnerability and risks associated with electronic PHI that is transmitted or maintained by a medical device." This can obviously provide a useful means for communication and awareness about possible security holes.

That said, Schwartz cautions that such manufacturers should design and create products that are "securable throughout the product lifecycle" and that they must be "mindful that there is an active adversary and that the device will need to be updated on a continuum so that it can be secure." She went on: "We recognize that device vulnerabilities may be that point of entry, that vector for access to the greater network, even while the device may remain unaffected—and that can put PHI and PII data at risk."

Slabodkin went on to point out a recent alert issued by the US Food and Drug Association regarding a computerized infusion pump "which communicates with hospital information systems via a wired or wireless connection over facility network infrastructures - that has serious cybersecurity vulnerabilities that could put patient safety at risk. The agency advised healthcare facilities to disconnect the pumps from their networks to reduce the risk of unauthorized system access."

Share and Share Alike

Amidst this growing array of threats to healthcare organizations, there is a very promising trend of sharing threat intelligence, and not just from software vendors to their clients, but amongst

and between healthcare organizations. In a recent article for *HealthCareITNews.com*, author Jack McCarthy quoted Denise Anderson, executive director of the National Health Information Sharing and Analysis Center (NH-ISAC). "Information sharing gives everybody the opportunity to see the threats that are out there and to protect against them," she said.

Anderson went on to explain some specific benefits of sharing such intelligence: "I can block this IP address at my perimeter so it doesn't affect me, or I can be making sure everybody is protected against this malware or is able to block this out so it never gets to the end users. So others have the opportunity to see the threats that are out there and protect against them."

Don't Fail to Plan

Almost all security experts agree that the threats to healthcare organizations are so vast, and so sophisticated, that the question is no longer whether, but when a breach will occur. That's why a response plan is critical for any responsible security team. Several key points should be considered:

- An Incident Response Plan will prepare an organization for the step-by-step process that gets employed any time a data breach or privacy incident is detected
- The IRP should take into consideration the magnitude of the breach, and focus on determine which specific systems and data sets were likely affected
- A specific team of professionals should be designated as members of the rapid response team; for each role, there should be at least one back-up, just in case the point person is unavailable when an event occurs
- Each step taken as part of a response should be documented, such that an analysis of the plans effectiveness can be made, post-event
- Every layer of the information architecture should be addressed in the plan: physical, network, software applications, servers, data, devices and users.

For more information:

Protecting Data & Lives with a Cloud Security Roadmap

http://pages.marketing.healthdatamanagement.com/20151111_hdm_clearda-ta_ws_lp.html?lg=20151111_hdm_clear-data_ws

Articles Quoted:

FDA Warns of Cyber Threats to Networked Medical Devices

Greg Slabodkin - NOV 11, 2015

http://www.healthdatamanagement.com/news/FDA-Warns-of-Cyber-Vulnerabilities-from-Networked-Medical-Devices-51539-1.html

The secret to stopping hackers? Share intelligence

Jack McCarthy - Nov 10, 2015

http://www.healthcareitnews.com/news/how-sharing-security-intelligence-stops-healthcare-hackers-privacy

A Hacker Identifies Glaring Holes in Network Security

Joseph Goedert - OCT 2, 2015

http://www.healthdatamanagement.com/news/Tips-from-a-Hacker-to-Improve-Network-Security-51347-1.html

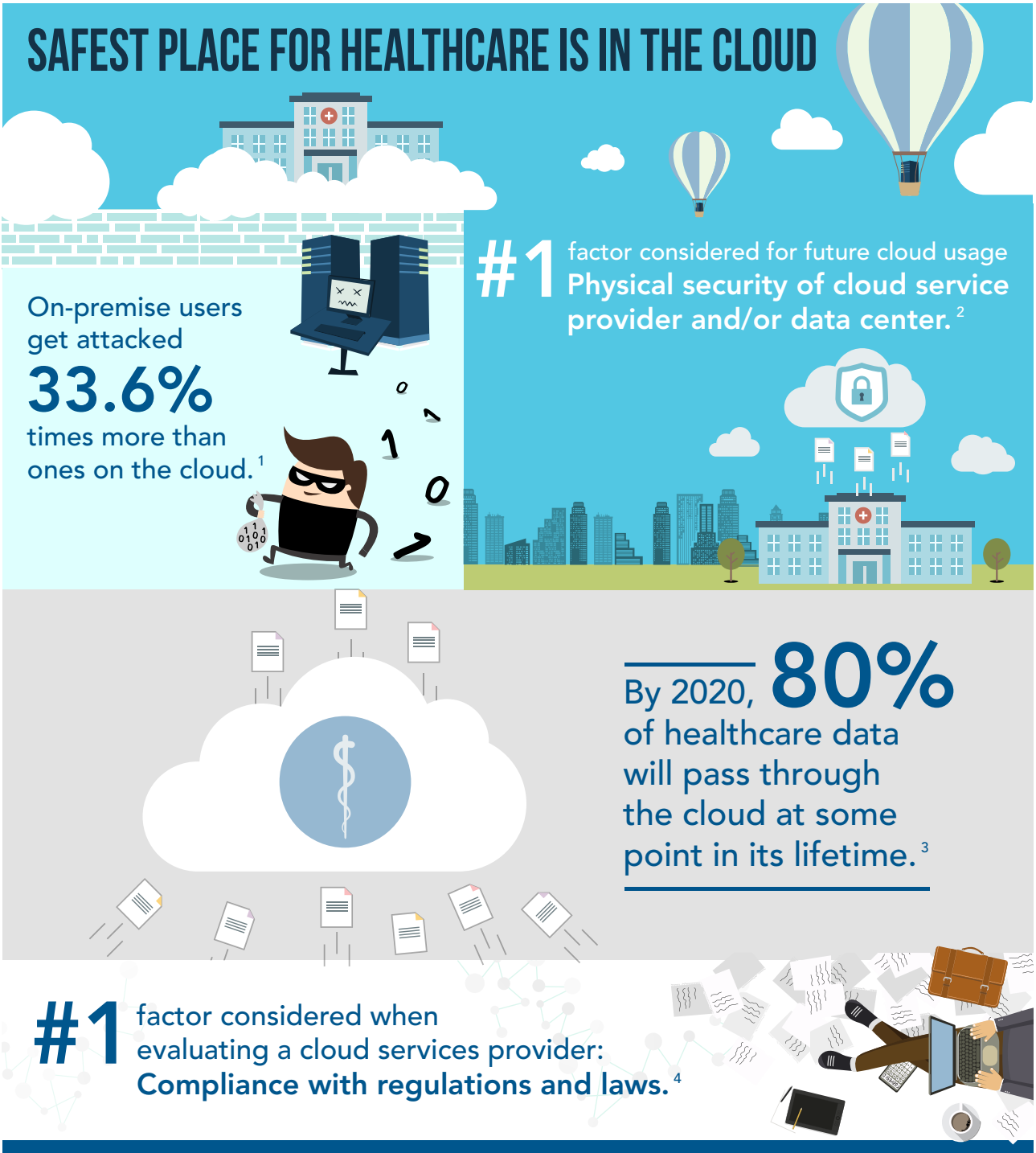
Risk Assessment

Part and parcel to a holistic security program is a detailed risk analysis. Bowen cautions that the Security Rule outlined in the Health Insurance Portability and Accountability Act (HIPAA) should be treated as the bare minimum. The risk assessment should assess potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI, so that all relevant assets can be protected.

Understanding the potential risks that face an organization can help decision-makers appreciate the level and type of investment that will be necessary to achieve a satisfactory security profile. Without such a framework in place, deciding where and how to invest time and energy becomes a more nebulous practice, which does not bode well for avoiding serious breaches.

For more information, call (800) 804-6052 or visit www.ClearDATA.com

Continue Learning



Learn more about Healthcare Security in the Cloud:
https://www.cleardata.com/whitepapers/the-safest-place-for-healthcare-is-in-the-cloud/

Sources:

1. *Removing the Cloud of Insecurity: State of Cloud Security Report," Alert Logic*
2. *Spiceworks survey of 100 U.S. IT professionals in healthcare, on behalf of CLEARDATAtm, January 2015*
3. *IDC Health Insights, November 12, 2014*
4. *HIMSS Analytics Cloud Survey, HIMSS, June 15, 2014*

ClearDATA
SECURE • HEALTHCARE • CLOUD

About Us

ClearDATA is the nation's fastest growing healthcare cloud computing company. More than 310,000 healthcare professionals rely on ClearDATA's HIPAA compliant cloud computing platform and infrastructure to store, manage, protect and share their patient data and critical applications.

For more information

101 West 6th Street, Suite 310, Austin, TX 78701, United States

(800) 804-6052

www.cleardata.com

ClearDATA
SECURE • HEALTHCARE • CLOUD