The C-Suite Battle Plan for Cyber Security Attacks in Healthcare

"If you know your enemy and you know yourself, you need not fear the result of a hundred battles."
– Sun Tzu, The Art of War

The heart of the tension between security and efficiency is the key vulnerability within your healthcare organization’s cyber security policy: employee passwords.

Cyber space is the modern frontier and cyber security is the modern healthcare organization’s most treacherous battlefield. Data is one of your most precious resources and your attackers will do anything they can to get their hands on it. In 2014 alone, a record-breaking 47% of American adults had their data hacked.[1] The landmark Anthem attack has drawn intense scrutiny and pressure on the healthcare industry, highlighting healthcare as a high-risk target.[2] And the FBI has issued a private industry notification warning that healthcare systems suffer an acute risk of cyber attack for financial gain and are more vulnerable to attack than financial and government sectors.[3] Patient’s private health records now fetch higher black market prices than stolen credit card on the black market.[4] This reality is fueling an unprecedented number of fraudulent insurance claims, identity thefts, and a growing number of attacks targeting healthcare organizations.

As a healthcare cyber security leader, you need advanced defensive strategies to protect your organization’s data from attack. And you need technological and managerial strategies to resolve the tension between data security and employee productivity within your healthcare organization. This tension is singularly important in the healthcare industry because hospitals need to strike a delicate balance between strong security and usable systems that enhance patient care without barricading patient information in inaccessible vaults. This security tension often breeds frustration, time wasting, and inefficiency for your clinical staff, particularly in light of the restrictive HIPAA, HITECH and Meaningful Use requirements that you are constantly being measured against.

The heart of the tension between security and efficiency is the key vulnerability within your healthcare organization’s cyber security policy: employee passwords. These passwords can be phished easily from even the most well-intentioned and well-educated clinical or administrative employee, as spear phishing attacks have become so sophisticated that they are now practically impossible to avoid. This whitepaper offers cyber security leaders in the healthcare industry proactive managerial and technological strategies to combat the danger of passwords within their organization, and tools to understand and engineer the social behaviors of clinical staff that hackers prey upon so successfully.

[1] CNN Money Report in association with The Ponemon Institute, http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/

[2] For a flavor of the coverage please see http://www.healthcareitnews.com/news/anthem-hack-healthcare-target

[3] FBI PIN # 140408-009 for the Healthcare Industry, https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf

[4] ‘Your medical record is worth more to hackers than your credit card’ by Caroline Humer And Jim Finkle http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

Your Plan of attack

"The most vulnerable component of any computer system is humans."

- Dr. Jane LeClair,
COO for the National Cyber security
Institute at Excelsior College,
Washington D.C.[5]

Know Your Enemy

CIOs have responded to the recent spate of cyber breaches in the healthcare industry with admirable acuity: they have re-secured their perimeter defenses and have cracked down on their password security requirements with gusto. Many organizations have built very strong perimeters, the strength of stone that can withstand powerful distributed denial of service (DDOS) and other brute force attacks.[6]

But, these walls will fall if CIOs do not acknowledge a hard truth: perimeter defenses are no longer the most likely target of an attack. Gatekeepers are. Employees are the gatekeepers of your healthcare organization's defenses and they are the most dangerous and vulnerable element of your cyber security shield. IBM cyber breach research reveals that C-level executives identify their employees as the single biggest threat to their organization's security.[7] Why? Because employees are people, people who use passwords. Their passwords are the keys to your perimeter and they can be easily stolen through social engineering schemes that prey on the most unmanageable elements of human nature.

No matter how well intentioned or intelligent your employees are, they can be easily manipulated into revealing their passwords through ingenious hacking attacks. Just as the walls of Troy fell to the trickery of the Greek's Trojan horse, and the Great Wall of China was continually infiltrated through gatekeeper bribery, employees fall prey to the trickery of well-disguised hacking schemes designed to exploit their trust. Phishing, spear phishing, and whaling attacks pinpoint their targets on employees' backs. These attacks manipulate employees to reveal their passwords through camouflaged emails from IT administrators, fake electronic medical record dialog boxes, and duplicitous upgrade packages.

It only takes a single click, or a simple password entry to unravel an entire hospital's security. As the legendary breaches of Troy, the historical breaches of the Great Wall of China, and the recent high-profile Anthem attack suggest, the strength of your perimeter is secondary to the security of your gates and how carefully your gatekeepers protect their keys. After all, the walls of Troy stood unbreached for 10 years before the Greeks turned their efforts to social engineering. Similarly, the recent Anthem attack exploited employees' trust and extracted their passwords through various social engineering techniques that brought Anthem's perimeter tumbling down, regardless of its strength.[8]

[5] 'Is Human Error Biggest Cyber security Vulnerability?' by Mike Lesczinski, http://news.excelsior.edu/human-error-biggest-cybersecurity-vulnerability/

[6] The top three areas of spending post breach include Security incident & event management, End-point security, and Intrusion detection & prevention, according to the Ponemon Report, 2014: A Year of Mega Breaches, http://www.ponemon.org/local/upload/file/2014%20The%20Year%20of%20the%20Mega%20Breach%20FINAL_3.pdf

[7] IBM: Quantifying the data breach epidemic, http://www-935.ibm.com/services/uk/en/it-services/data-breach/data-breach-statistics.html

[8] For further coverage on the details of the role a stolen employee password played in the Anthem hack, please see http://www.fiercehealthit.com/story/details-emerge-anthem-hack/2015-02-06

This whitepaper examines the most common social causes of password vulnerabilities that negate healthcare organizations perimeter defenses. It is designed to help cyber security leaders to identify, understand, and re-engineer these weaknesses into security strengths by employing a key strategy that military leaders and hackers live by: know your enemy and know yourself. For, when it comes to organizational cyber security in the healthcare industry, your organization is its own worst enemy. Your human perimeter is the key to your survival: an accidental move by a single member of your organization's hierarchy can put your entire healthcare facility in jeopardy.

Know Yourself

The best way to protect your healthcare organization from an employee password attack is by thinking about your organization like a military attacker or a hacker. Hackers perform meticulous research before they pounce on their prey. They can observe users' digital behaviors for weeks before they identify the most promising avenue for a successful social attack.[9] They need to understand the people they attack in order to trick them into revealing their secrets. The most proactive cyber security leaders follow suit: they perform meticulous self-evaluations of their organization's vulnerabilities, workflow problems, and cultural phenomena before devising the best form of defensive strategy to suit their organization's needs. You can do this by:

- Identifying the most likely forms of attack: the key employee behaviors and other factors that bring risk to your healthcare organization.
- Understanding why you are vulnerable to attacks: identify the contributing factors and workflow requirements that cause your clinical and administrative staff to favor risky behaviors.
- Eliminating your vulnerabilities' root causes: manage the root causes of risky employee behaviors by intervening with technological or social means.

The best way to protect your healthcare organization from an employee password attack is by thinking about your organization like a military attacker or a hacker.

[9] For further information about how hackers research their targets please see http://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/110/anatomy-of-a-data-breach

To avoid some of the risks of endpoint theft, many organizations in the healthcare industry are transitioning to virtual desktop infrastructure (VDI) environments that support thin and zero clients.

Identify the most likely forms of attack

Understand the most common battle plans
Analysis of major cyber security breaches suggest that your employees are the key vulnerability in every organization's IT security systems. In healthcare specifically, employees' password behaviors, log in work-arounds, general clicking patterns, and email-opening behaviors breed numerous vulnerabilities. These risks present themselves in a variety of situations that cyber attackers exploit in specific ways. Here are some of the most common examples:

Phishing
Phishing is the blanket term for masquerading attempts designed to extract user information, passwords, credit card numbers or other sensitive information from electronic communications (most commonly, emails).

Spear phishing
Spear phishing is a more targeted and personalized form of phishing, through which scammers attempt to extract information from individuals by sending fake emails from people or businesses they know or trust. Spear phishing thrives on familiarity and trust of personal relationships and job duties.

Whaling
Whaling is a form of spear phishing that targets 'big fish': high-ranking executives and employees with advanced access to their organization's computer system. Key targets include the CIO, CSIO, EMR administrator, and members of your Access Control Office and medical credentialing teams.

Lost devices/hardware
Device theft and loss still pose significant risks for healthcare organizations that keep sensitive data on endpoint devices and on their own mobile devices (an increasing trend, with the transition to progressive Bring Your Own Device (BYOD) policies in the healthcare sector). To avoid some of the risks of endpoint theft, many organizations in the healthcare industry are transitioning to virtual desktop infrastructure (VDI) environments that support thin and zero clients.[10]

Unencrypted password lists
Oftentimes password-fatigued healthcare employees will keep unencrypted text files containing their EMR passwords on their computer, or leave sticky notes with various application passwords in plain sight on their keyboards, lab walls, or shared workstations. Full-disk encryption can help assuage the risks of unencrypted documents, but little can be done to defeat the low-tech sticky note hack.

[10] The Imprivata 2014 Desktop Virtualization Trends in Healthcare Report revealed that 84 percent of survey respondents indicate their organization will use SSO within their VDI environments within 24 months. http://pages.imprivata.com/rs/imprivata/images/Imprivata-2014-Desktop-Virtualization-Trends-in-Healthcare-Report.pdf

Test your own boundaries

Some CIOs extend the lessons about the danger of employee-related errors that high-profile hacks teach by performing their own internal penetration tests. These tests mimic the key strategies hackers employ to dupe employees.[11] Often, they return disappointing results. Some CIOs in leading hospitals who Imprivata management have spoken with have reported successful penetration rates of 30% or more. Similar results have been reported by McAfee, whose Phishing Quiz results indicate that 80% of the 16,000 business users they targeted with fake phishing schemes succumbed to at least one phishing attempt.[12] Furthermore, the McAfee results revealed that the employees in departments holding the most sensitive data (Finance and HR) performed the worst, by a significant margin. These results are shocking, given the fact that a single employee error is all that is needed to breach a healthcare organization's security. Regardless of the results of your internal penetration testing, the exercise will be extremely useful to you: it will offer you invaluable knowledge of how vulnerable your organization is to specific forms of employee-targeted attacks, and whether you need to double-down your efforts in particular departments, application users, or specific clinical workflows.

McAfee Phishing Quiz results indicate that 80% of the 16,000 business users they targeted with fake phishing schemes succumbed to at least one phishing attempt.

Understand why you are vulnerable to attacks

It is not enough to simply know what your weaknesses are. You need to know why your weaknesses exist in order to conquer them. So, in order to defend against your vulnerable employee behaviors, it's important to understand what the root causes of risky employee behaviors are. Here are some of the most common root causes in healthcare settings:

Too many passwords

Sometimes the answer to password-related breaches is simple: healthcare employees have too many passwords that they have to enter so many times each day that it becomes second nature to automatically enter their password whenever they see a prompt. HIPAA privacy regulations require frequent password entries, complex password chains, and frequent password changes. These requirements can cause a lot of employee frustration in high-stress clinical settings. They also lead to password recycling and sharing which are recipes for vulnerability, from a hacker's perspective. Even with more healthcare organizations integrating advanced, multi-factor authentication options to reduce password loads, the increase in SaaS applications will only continue to add to the heavy password burdens of employees in the future.

[11] For further information and guidance on penetration testing approaches please see http://www.sans.org/reading-room/whitepapers/testing/penetration-testing-alternative-password-cracking-35717

[12] McAfee Labs Threats Report, August 2014, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2014.pdf

In shared desktop settings there is little sense of personal ownership, or responsibility for computer usage.

Too little knowledge
Oftentimes healthcare employees are simply unaware of how targeted and camouflaged hacking attacks can be. Clinical staff, in particular, are unaware of the evolving risks in the cyber security space because they are constantly under siege with rapid-response healthcare situations, emergency treatments, and patient care needs. Most healthcare employees know not to click on links in suspicious emails claiming to be from members of a foreign royalty, but they are less aware of the risks of malware, Trojan horses, or spear phishing schemes that can hijack their clinical applications.

Too much to remember
The average healthcare employee has to use dozens of different, complicated passwords to log into their EMR systems and clinical applications. Strong HIPAA password requirements lead to huge numbers of passwords, which in turn breed high instances of forgetting those passwords. Many members of your clinical workforce may resort to writing their passwords down in notebooks, unencrypted word files, or sticky-notes they leave on their computer, in order to avoid the frustrations of forgetting their passwords and being locked out of their account.

Too many people
Shared workstations are particularly prevalent in healthcare organizations and more and more healthcare facilities are transitioning toward Virtualized Desktop Infrastructure (VDI) environments. In these shared desktop settings there is little sense of personal ownership, or responsibility for computer usage. This diffuses the responsibility and accountability for keeping tabs on the security settings of individual computers and can lead to risky account sharing; accidental overwrites of other people's settings, and exponentially increased login requirements.

Too little time
Oftentimes clinical employees simply don't have enough time to log out of their computer when they're called away to the ER, or to pause and consider the validity of a password prompt when they're treating an urgent patient injury. Clinical staff work in one of the highest-stressed and time-pressed industries. And, they often share passwords with their team members to mitigate the added layer of stress that IT security layers to their myriad responsibilities. They may also leave a workstation open and logged-in to save precious time that never-ending log in and log out processes cost them, and their patients, during their clinical workflows.

Eliminate your vulnerabilities' root causes

Once you identify the heart of your employees' vulnerable behaviors, consider patching these weaknesses with technological means. Instead of exploiting the vulnerabilities, as a hacker would, you can defend your vulnerabilities by engineering your healthcare system so that its vulnerabilities are diminished, or eradicated by changing employee behaviors through targeted technological and educational methods that tackle the heart of your organization's security problems.

Because healthcare employees' vulnerabilities to hacking attempts are so complex and numerous, educational methods will not be able to win the battle for security when used in isolation. Spear phishing schemes can be so sophisticated that they can even dupe cyber security experts. Some spear phishing schemes even require detailed technical analysis to identity whether they are legitimate, or spurious - something which typical employees do not have the knowledge, or time to discover on their own. So, in order to best avoid a security breach, technological intervention is your best approach:

Without addressing the root causes of your employee's password problems, your attempts to secure your healthcare facility from the risks of an employee-related breach will fail.

Consolidate all your keys into secure master keys

The root cause of employee-error breaches can be boiled down to a simple trifecta of problems:

- Healthcare employees have too many passwords
- Healthcare employees have to type and click too much when entering their various passwords
- Healthcare employees have to enter passwords too often

These problems are exponentially exasperated in VDI environments with shared workstations that require additional authentication and access requirements to roam successfully across devices. Without addressing the root causes of your employee's password problems, your attempts to secure your healthcare facility from the risks of an employee-related breach will fail - as will your attempts to leverage the full potential of your VDI investment.

Your employees' domain passwords have the potential to throw open the gates of your perimeter to anyone who uses them. But you can effectively lock those gates and throw away the majority of your keys by using a single sign on solution. Imprivata OneSign® Single Sign-On is the perfect tactical solution for your security strategy: it eliminates passwords, eradicates time-consuming sign ins, and - most importantly of all - it saves your clinicians much-needed time.[13] An effective single sign on solution addresses the heart of your employee's risky password behaviors with a dual-pronged defensive

[13] Imprivata OneSign has been shown to save clinicians up to 45 minutes per shift. For more information please see the Mahaska Health Imprivata Customer Success Story: http://www.imprivata.com/sites/default/files/02-2014-Mahaska.pdf

Passwords are difficult to eradicate completely in the healthcare industry.

strategy: it satisfies employee's understandable impulses to save time and increase convenience and it increases security, without adding extra complications for your clinical staff's workflows. It's extremely unusual to find an organizational solution that simultaneously increases security and convenience in healthcare settings - but an effective SSO solution does exactly that. It's a win-win security strategy.

Lock down your master keys

As experienced cyber security leaders know, passwords are difficult to eradicate completely in the healthcare industry, even when you add a single sign on solution to your security arsenal. Many important clinical computer applications require copious password entries (they're written into the DNA of the majority of EMR programs, for example). That's where Imprivata OneSign Authentication Management comes in: a system that allows your employees to enter strong passwords automatically, with a tap of their badge or swipe of their fingerprint. At the start of their work shift, they log in with a password or pin, and for the rest of their shift they just need to tap or swipe in to automatically populate their passwords and access their clinical applications.

With an authentication management solution, employees still use multiple passwords, but they don't have to know, remember, or enter all of them manually. Effectively they're still using (and carrying) a set of keys, but they can't share them with malicious attackers, because it's impossible for them to share information they do not have direct access to. Instead, they use their passwords indirectly and securely. A properly architected authentication management system can't be as easily tricked to divulge passwords secrets like a person can be: it won't populate passwords for fake dialog boxes and it won't store or share passwords in unencrypted file types. Instead, it locks employee passwords and patient health records down in a convenient, usable format: an automatic technology that's very difficult to trick and impossible to engineer socially.

Educate your gatekeepers

Once you eradicate, or vastly reduce your password requirements with Imprivata OneSign Single Sign-On and Imprivata OneSign Authentication Management, your educational strategy for reducing the risk of employee-related hacks becomes very simple. All you need to say are "You never have to enter your password manually because IT has already enabled all of your necessary applications." Employees will know that if they're prompted for their password, something is wrong, and they'll be able to easily red flag the issue for your IT team. Even better, you can configure your system so that your employees won't be able to manually enter their password, even if they wanted to, because they don't know their password strings.

Win Your War

The key to your defensive strategy lies in your ability to understand the unique needs of your organization and your ability to observe and manage your employee behaviors and clinical workflow needs in an insightful way: a way that works for them, not against them. This insight is the crux on which many a battle result has balanced, and one which can be easily tipped in your favor by employing the right technological and managerial strategies for intervening in your troops' defense. By actively considering the needs and vulnerabilities of your human perimeter you are sure to become a more effective and successful cyber security leader. Why? Because the best leaders never fail to identify, consider, and protect their weakest links. And, even though the battlefield of cyber security is constantly changing, and the lines of defense are constantly shifting, the secret weapon of success will forever continue to be the qualities of leadership that you can provide, paired with the help of ancient war advice and the latest technology.

A strategic partnership

When it comes to winning the myriad battles in the field of cyber security the most decisive and valuable lieutenant will be a partner that understands your specific healthcare needs, acknowledges your clinical workflow weaknesses, and empowers your organization to succeed despite its vulnerabilities. An SSO solution proves the perfect partner in such circumstances because it harnesses your specific organizational weaknesses into strengths. To learn why Imprivata is the SSO vendor of choice in the healthcare industry visit www.imprivata.com to read more and schedule a demo to suit your specific organizational needs.

> By actively considering the needs and vulnerabilities of your human perimeter you are sure to become a more effective and successful cyber security leader.

imprivata®

About Imprivata

Imprivata (NYSE: IMPR), the healthcare IT security company, is a leading provider of authentication and access management solutions for the healthcare industry. Imprivata offers single sign-on, authentication management and secure communications solutions that enable fast, secure and more efficient access to healthcare information technology systems. Imprivata solutions address multiple security challenges and improve provider productivity for better focus on patient experience.

For further information
please contact us at:
1 781 674 2700
or visit us online at
www.imprivata.com

Offices in:
Lexington, MA USA
San Fransisco, CA USA
Santa Cruz, CA USA
Uxbridge, UK
Paris, France
Nuremberg, Germany
Den Haag, Netherlands