DP Solutions
Problem Solved.

Protect Your Practice

Lessons Medical Practices Can Learn from the Target Data Breach to Manage Risk, Meet Compliance Standards and Safeguard Their Organization

Read This Whitepaper and You'll Discover:

- ✓ What Medical Practices Can Learn About HIPAA/HITECH Compliance from the Target Data Breach
- ✓ 4 Things Medical Practices Can Do To Protect Patient Data and Ensure the Integrity of Their Practice
- ✓ 7 Easy Steps You Can Take Today to Manage Risk for Your Medical Practice
- ✓ How You Can Uncover Any Vulnerabilities Your Practice is Facing and Correct Them to Meet Compliance Standards

By Ben Schmerler
vCIO Consultant
DP Solutions

4 Lessons Medical Practices Can Learn About HIPAA/HITECH Compliance from the Target Data Breach

In late 2013, Target customers who shopped at their stores all across the United States were unwittingly giving their sensitive, personal data to hackers as part of a comprehensive attack that may have been avoidable. Customers assumed they were doing business as usual. They expected that Target was keeping their transactions and exchange of information confidential between two trusted parties. Sound familiar?

Any professional organization, like a medical practice, engages in complex transactions of money and information on a daily basis. In the case of medicine, this is even more extreme, since this flow of data is not only between the patient and doctor, but the doctor's employees, insurance companies, pharmacies, and other business associates. The data itself isn't just financial, but sensitive medical information. Medical practices and patients are held to an entirely higher level of trust than a retailer and its customers.

In this white paper, we discuss the circumstances surrounding Target's data breach in an effort to first educate those who are interested in understanding how something like this could happen. Then, we will talk about lessons from the Target hack and how your medical practice can avoid the consequences of potential data breaches. We'll wrap things up by letting you know the steps you can take to ensure your practice is compliant and protected.

So what happened to Target? How does such a large company that must have invested significant dollars in technology, let 40 million credit card numbers get taken from their Point of Sale (POS) system?

Retailers like Target, who take credit card numbers frequently, have to meet PCI compliance to ensure that, at the POS system, transactions are secure. Target met this required compliance standard in an attempt to avoid credit card fraud and other hacks on their electronic systems. However, hackers installed malware on the POS system itself, which was the root cause of the breach. Customers were completing transactions at the registers while unknowingly transmitting their personal information to someone who wasn't entitled.

This malware was installed through a backdoor. A "port" on the network, which was open for legitimate traffic to go in and out of Target's corporate network, was exploited. It's believed that login credentials for a third party vendor of Target were cracked, allowing hackers to get in with those credentials and giving them access to not only what the vendor had rights to, but to the POS system itself. The malware

was installed and the data was collected in an area the hackers set up within Target's own system for them to take.

Making matters worse, this happened over the course of several weeks. The initial attack to break into the system was successful, the malware started running, and the hackers were able to continue to exploit their access to Target's system and literally harvest data for what appears to be the purpose of committing large scale credit card fraud through a foreign country. These hackers clearly had access to more personal information associated with these credit card numbers, like addresses, names, purchase information, etc. The extent of the total data breach doesn't appear to be known. The credit cards were just the smoking gun.

Target failed to react to alerts on their own system, which was designed to catch these sorts of attempts before they became major breaches. There was a failure of management to evaluate what levels of risk they could tolerate before making changes to the security polices of the company. Because of this, Target faced serious consequences. The financial cost was comprised of a massive amount of fees, fines, and purchases of credit monitoring services for millions of customers throughout the country. Sales were lost, as customers chose (whether justified or not) that their money and information was safer with Target's competitors. Their brand had been tarnished to a large degree, and that may or may not be reparable.

How does this apply to me? If Target can't protect themselves what can I learn from a practical sense to protect my practice and my patients?

Let's break down a few key things that you should remember moving forward as technology continues to become a greater part of medicine.

▶ Lesson #1: Pay for Prevention Now, or Pay for the Consequences Later.

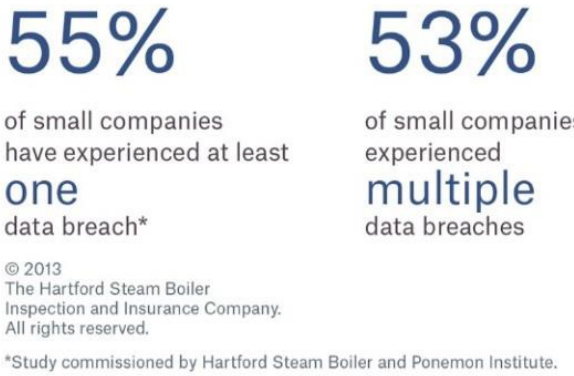
It's safe to say that even though Target met PCI compliance, they weren't doing all they could to prevent this kind of attack from happening. Clearly they could, and should have, done a periodic review of the security policies as it pertains to access and user rights. They didn't appear to know (or possibly, weren't diligent enough to realize) that through a third party vendor, that had nothing to do with credit card transactions (an HVAC contractor), there was a loophole that allowed far more access into deeper and more sensitive data. In the case of the third party vendor whose credentials were exploited, they also likely failed to have a coherent business agreement as it pertains to the use of technology.

Let's not forget to mention that the malware prevention on the POS system itself was inadequate. PCI compliance, while met and certified, ignored the fact that the malware prevention software was older

and not up to date. The attack on the POS system was from a known piece of malware floating around the hacking community prior to this attack. Infection could have been avoided from multiple levels.

Lesson #2: Technology is Very Important. But Management is Equally Important.

Even if Target had more sophisticated security measures to prevent these attacks, it appears that key decisions were not made, something that Target's own spokespeople have admitted. Target had a monitoring solution in place to evaluate various threats and alert an information security team to react and make decisions. It appears that their team believed that these threats didn't warrant any further action. This key decision singlehandedly took a minor security issue that was fully controllable and resolvable, and turned it into a corporate crisis.



It's simply not enough to have a security solution in place if the people working with you to manage and maintain this solution aren't analyzing and evaluating information in real time. Threat levels change constantly, and it takes significant diligence and policies to create a culture of data protection.

Lesson #3: It's Not Just Target. This Kind of Attack is Cheap and Accessible. It Doesn't Matter Whether You're Big or Small.

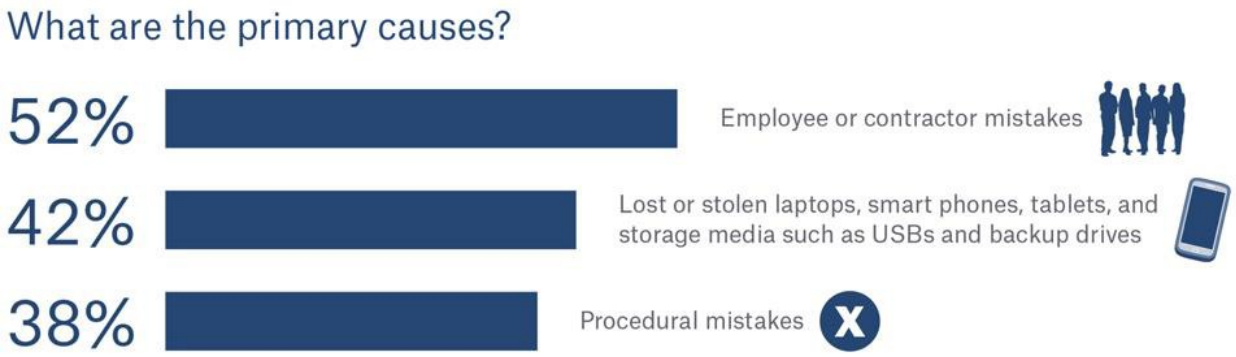
The malware that was used for this attack is accessible on the Internet. Anybody who has the knowledge and the desire can use tools that are easily available to perform similar attacks.

While Target made the big headlines, several other smaller retailers and credit card accepting businesses were hit with similar attacks.

Although the details of these attacks weren't as publicized, it appears that there were several common threads, including similar vendors, software, policies, etc., even if it wasn't on the same scale.

Given the relative ease for someone with limited resources to engage in a sophisticated attack to hijack your data, it doesn't take that much of a return in order to justify making the attempt. Even in a small organization like a medical practice, there is enough valuable information to make it worthwhile for someone to want to take your data. These hackers are looking for the easiest targets for successful attacks. If you go online and investigate for yourself, you will discover that the medical practices that have been forced to disclose their data breaches vary from small medical offices with only a few doctors, to large hospitals with large amounts of patient data.

Lesson #4: Compliance and Risk Management for Technology is Manageable, Just Not by One Individual.



*Study commissioned by Hartford Steam Boiler and Ponemon Institute.

While Target failed on several levels to execute a technology security plan, the good news is, that even in small organizations, there are very reasonable steps that you can take in order to handle both Compliance and Risk Management. Certainly nothing is 100% secure and protected as every day new threats come along that can harm any device that connects to the Internet. Not only that, but some of the greatest threats to your practice can come from mismanagement and a lack of understanding as it pertains to protecting the practice's data.

The goal for your practice has to be minimizing that risk. Your employees, vendors, and security partners must work together to ensure security is valued and enforced.

While HIPAA/HITECH demands a Compliance Officer, even the best Compliance Officers don't know everything. A full security plan has to take into consideration how the practice works, with data flowing internally and externally to employees and third parties. It has to consider what technology solutions are in place and how often those solutions are reviewed and maintained. These plans must include a full understanding of how the system can be accessed, and limiting that access only to what is absolutely necessary. And while automation is nice and important, decisions need to be made along the way by knowledgeable people so that the system and process works as designed.

A great Compliance Officer manages the process and brings everyone together to create cohesiveness and reduce risk. That's why Compliance Officers should seek out valuable partners who share the culture of data security that the practice wants to have both for themselves and their patients.

6 Easy Things You Can Do Now to Manage Risk

As a Practice Manager, or a doctor who owns their own practice, there are a few key items you will want to address to fortify your organization.

1. **Strengthen your system defenses**
   One of the foremost steps you must take to protect your practice's data is to implement strong computer defense systems. This means putting basic security measures in place such as a robust firewall, email and text encryption, up-to-date anti-virus and anti-malware software, patch management, and a good web filtering application. Starting with these basics will give you a solid foundation upon which to build.

2. **Assess risk & identify weaknesses**
   Many compliance standards require regular risk assessments to identify any issues that may be present in the information security infrastructure. By performing regular risk assessments, you can often catch small problems before they become big problems.

3. **Educate employees**
   Training is critical to maintaining a secure computing environment. Without training, users may compromise data through ignorance of an established policy or procedure, or fail to notify the appropriate personnel of a suspected or confirmed breach.

   Administrator training helps prepare the local administrator to deal with the most common security related issues that may arise on a day to day basis, while user training is focused on security best practices including basic information security and strong password selection.

   To ensure staff members are doing their part to maintain a secure practice, employees should be taught to:

   - Value the security of the organization's assets
   - Handle sensitive data with extra special care
   - Beware of scams & fraud - think before you click and err on the side of caution
   - Keep operating systems and software up-to-date
   - Avoid installing unnecessary programs on devices
   - Have an active awareness of security

4. **Create strong passwords & keep them private**
   A few basic guidelines will ensure that employees adhere to password best practices to thwart security breaches. Passwords should:

   - Be at least 8 characters long
   - Not contain user name, real name, or company name
   - Not contain a complete word
   - Be significantly different from previous passwords
   - Contain a combination of uppercase, lowercase, numbers, & symbols

5. **Guard data & devices when you're on the go**
   Security standards shouldn't go by the wayside when you are not in the office. When you're working remotely on mobile devices, it's especially important to keep the mobile security guidelines in mind:

   - Make sure to use secure connections
   - Encrypt confidential data
   - Save sensitive activities for trusted connections
   - Open attachments carefully

6. **Back up important files**
   You never know when you'll need to restore data, but you have to be ready at all times. The best practice is to store your data onsite, with a complete, fully encrypted copy in a totally secure offsite location.

How Do I Get Started to Ensure My Practice is Protected?

Understanding the assets your practice has, the security guidelines that are in place, and areas of vulnerability or weakness are the first steps protecting your practice. You need to have a firm awareness of where you are in order to get to where you need to be.

DP Solutions' **Comprehensive HIPAA Assessment** provides a thorough evaluation of your practice as it relates to areas of compliance. Working with over 150 medical practices across the Mid-Atlantic for over 10 years, our Compliance & Security Specialists have developed processes and strategies that help medical practices address and remedy their security and compliance concerns.

During the Compliance Assessment, our one of our Security Specialists will come to your office to evaluate:

- What are the largest threats to the security and integrity of your critical patient and practice data?
- What backup, security and business continuity systems you currently have in place and determine whether they are sufficient.
- Is all of your critical practice and patient data being backed up, every day?
- Do you know what steps and costs would be involved to bring your practice up to current compliance standards?
- How prepared would you realistically be in the event of a compliance audit?
- How can you maintain an ongoing security and compliance discipline for your practice?

After the assessment, you will receive a thorough, easy-to-understand Assessment Report outlining where your vulnerabilities are and what steps your practice needs to take to be compliant. We will review these findings with you and address any additional questions, concerns and potential next steps.

Here are a few additional reasons you will want to take advantage of a Comprehensive HIPAA Assessment:

- ☑ Clarify complex standards into easy-to-understand action items for your practice.
- ☑ Educate management about proper HIPAA standards as it pertains to your specific situation.
- ☑ Understand the effectiveness of your security protocols and maintenance for your IT resources.
- ☑ Position your practice as one that has taken “due diligence” when it comes to HIPAA, and not giving it lip service.
- ☑ Uncover specific threats and risks to your practice.
- ☑ Meet a key Meaningful Use requirement, which requires practices to conduct a risk assessment and correct any identified deficiencies.
- ☑ Confirmation and/or discovery of the locations of sensitive data on your network in order to better manage “data sprawl”.

- ☑ Ensure that your staff has the proper level of access to the system to help adhere to the "Minimum Necessary" HIPAA standard.
- ☑ Reinforce a culture of security throughout your organization to protect ePHI.
- ☑ Allow your team to focus on the management of the practice instead of figuring out standards that may be unfamiliar to them.
- ☑ Develop a long term plan for the evolution of your technology that touches ePHI.
- ☑ Avoid surprises of potential security flaws that could have been mitigated in advance.
- ☑ Understand the value of specific measures to help manage risks.
- ☑ Avoid data breaches that can lead to hefty fines and loss of license.

Does Your Practice Need A HIPAA Assessment?

If you're unsure if a Comprehensive HIPAA Assessment would benefit your practice, then a FREE Security & Compliance Consultation will get you headed in the right direction.

At no cost, one of our Compliance Specialists will spend 30 to 60 minutes with you to:

- Learn about your practice's specific goals & objectives
- Understand how your practice is addressing compliance
- Review your concerns around security risks and exposures
- Discuss options and outline steps to remedy any risk factors

Since this is free, you have no good excuse not to do it now. If we don't find any problems, you will at least have peace of mind that your compliance and security efforts are up to par and that you could properly handle a compliance audit. But if we DO find any shortcomings, you'll be able to fix them BEFORE you're audited.

Claim Your Free Security & Compliance Consultation Today at www.dpsolutions.com/ComplianceOffer or by calling 410-720-3300 x2

About the Author

Ben Schmerler is a vCIO Consultant at DP Solutions, one of the most reputable IT managed service providers (MSP) in the Mid-Atlantic region. Ben works with his clients to develop a consistent strategy not only for technical security, but also policy/compliance management, system design, integration planning, and other business level technology concerns.

About DP Solutions

Simply put, the sole goal of DP Solutions is to streamline our clients' IT management, allowing them to grow their business. With over 45 years of experience, we serve as a trusted IT business partner to our clients. We provide innovative managed IT services, IT disaster recovery, and cloud business services that give our customers the peace of mind that their businesses will run efficiently, effectively and securely. DP Solutions is committed to excellence in our work ethic, in the products and services we provide, and in our relationships with our clients and communities. For more information, please visit, www.dpsolutions.com.

This report is provided as an educational service courtesy of

DP Solutions
Problem Solved.

9160 Red Branch Road, Suite W-1
Columbia, Maryland 21045
410.720.3300
www.dpsolutions.com
sales@dpsolutions.com