HEALTHCARE CYBERSECURITY PLAN

How to battle the world of cyberthreats without leaving it to chance

Netsurion™ EventTracker
Healthcare Cybersecurity Plan: How to battle the world of cyberthreats without leaving it to chance

Published in 2017 by Netsurion

On the web: www.netsurion.com

This eBook is the second in a series developed and released by Netsurion, a leading provider of managed security and compliance related services. The first eBook in the series focused entirely on basic training concepts as it relates to running and securing information technology systems. That first eBook can be accessed and downloaded from www.netsurion.com/cybersecurity101.
Executive Summary

Ignoring the issue is not worth the risk.
Cybersecurity in today’s healthcare world is complex. To start out with an analogy, you may recall the popular game of strategy, diplomacy, conflict, and conquest in which players control armies in attempts to capture territories from other players. The object is to occupy the 42 territories on the board, grouped into six continents. Although the rules are simple, there is complexity in the interactions throughout play. And as the game progresses, keeping track of your army while trying to make strategic moves and remain competitive can be overwhelming. The more players involved, the more chaos can ensue. The game requires strategy and planning to win, not just luck by dice; however, if all of those playing are good at the “game”, then it becomes more of an equal battle of wits, which means the winner’s fate is left to a roll of the dice.

For the C-suite of large systems of hospitals, office managers, and physicians running practices, healthcare challenges today can sometimes feel chaotic like the complex nature of this game. Each day may seem more hectic than the previous with visiting patients, emergency calls, demanding physician schedules, medical billing, coordinating with insurance companies, and keeping up with back-office logistics and record management...all while trying to offer great care in a competitive healthcare industry.
Bringing the severity of the situation home is the fact that each aspect of this challenging environment generates the need to collect a plethora of personal data, and there is always an adversary out there ready to out-strategize, and out-play you. Despite the confidential data medical organizations house, compliance and security are usually not top-of-mind in the field – their focus is on patient care, as it really should be. But part of that care is protecting patients’ personally identifiable information (PII) and protected health information (PHI). Yet in the end, too many healthcare providers and organizations leave things up to a roll of the dice.

Those medical forms we all fill out is fertile ground for criminals to steal identities. Most healthcare consumers know this, but do it anyway, trusting their provider to have all the right systems in place to protect their data. If patients lose trust about PII and PHI protection methods, they can lose trust in the overall care by providers.

In speaking with healthcare professionals over the years about how they protect patient information, their responses are always similar: “We have antivirus.” “We take HIPAA training every year.” “I think we have an IT guy for this.” “We have a few doctors and see about 50 patients a day, we are small, this won’t happen to us.”

Sure, it’s usually the healthcare giants that make the breach headlines, but just because hackers can mine larger troves of data from the big guys doesn’t mean smaller practices are in the clear. And let’s not forget those security breaches that occur due to an inside job. This could be a disgruntled employee, a lack of properly managed security and firewall, failover/downtime, or simply an accidental download by an employee that starts in one machine and infects an entire system if not caught in real-time.

The harsh reality is that many healthcare organizations and offices just aren’t ready to secure the territories and win the game against their crafty opponents. Although there are electronic medical record (EMR) safety measures built into the 1996 Health Insurance Portability and Accountability Act (HIPAA), the element of human error and the “it won’t happen to us” mentality gets in the way of real security. Plus, this Act doesn’t detail the real-world steps and security measures necessary to truly remain secure in today’s cloud-based world, it simply states you need to protect the data to remain compliant – but how? Cybercriminals are more than ready to swoop
In today’s world of ever-expanding Internet criminal activity and cyberthreats, now more than ever before, it is critical that we secure our networks as much as possible. The previous notions of lone hackers attacking critical systems has now become a myth and the truth is even more frightening.

In 2016, we began encountering larger groups of cyber criminals enacting coordinated attacks against corporations and even government institutions. Breaching a network is tough business, but defending one is even tougher.

The rule of thumb is that an attacker only has to be right one time and a security specialist has to be right every time. It is for these very same reasons that Netsurion recommends using every tool at your disposal to deflect these attacks and protect against these threats.

A good security plan can be overwhelming at first, but with the right knowledge and expertise, it can be simplified and managed to reduce the exposure of your practice or hospital and limit the amount of risk you might take.
How big is the problem?

The FBI warned healthcare companies in 2014 that their industry was not doing enough to resist cyberattacks, especially compared to companies in the financial and retail sectors, according to Christopher Budd of security software company Trend Micro. The warning came in a government bulletin to U.S. companies that cited research by a nonprofit security institute.

It is estimated that the healthcare industry is generally about 10 years behind the financial services sector in terms of protecting consumer information. It may be twice as easy for hackers to get sensitive financial information out of a healthcare company compared to a bank.

Cybercriminals know that physician offices are often not as secure as they could be, and that they still house sensitive medical, financial, and personally identifiable information. The proliferation of Electronic Medical Records (EMR), coupled with recent breaches of patients’ personal health information and personally identifiable information, has highlighted the need for security of medical office networks. While HIPAA does not specifically spell out the requirements necessary, it does mandate the need to place safeguards to protect patients’ health information. These requirements become increasingly complicated as more doctors want to offer Wi-Fi to their patients and employees.
Small organizations are impacted indirectly by criminals who target a major solution provider used by small practices; therefore, hitting many with one fell swoop.

There’s been an uptick in hackers using remote access points to get on the network. Attacks start through remote access vulnerabilities, then malware is introduced into the network through cross-site scripting, a common database vulnerability.

Below is a breakdown of some of the major threats to healthcare entities of all sizes:

**Malware**
Over 317 million new pieces of malware were discovered in 2014 alone. Constantly evolving and looking for vulnerable systems to latch on to, a managed firewall and security service will keep you ahead of malware threats.

**Employee Mistakes**
Lack of sufficient employee training and weak security controls frequently leads to mishandled data and easy targets for data breach. Having a security partner to provide employee training and security guidelines can eliminate this threat.
External Hacking

47% of all breaches in 2014 were caused by malicious external attacks. Maintaining a tightly configured managed firewall that is constantly monitored will enable you to detect and properly report data breach attempts.

Internal Hacking

Malicious abuse by a company insider accounts for almost 25% of data breaches. A managed firewall with circumvention detection ensures your security controls are always on and properly running.

It’s not uncommon for healthcare breaches to not be discovered for a while. As a comparison, when credit card data is stolen, banks will notice a large number of new transactions, and can begin to correlate that data through knowing that many of those customers all shopped at the same retail store within the past week. However, there’s no centralized market for stolen identities – there’s never going to be an external source similar to a bank, until the FBI gets involved. If you don’t have systems in place to monitor both in-bound and out-bound network traffic, you will have no idea who is on your network, or what is going on and you will just be pouring out data.
What will happen if my practice or organization is breached?

In addition to HIPAA requirements, if your practice or organization accepts any type of credit card payment, you are also responsible for adhering to payment card industry data security standard (PCI DSS) requirements. Each has its own set of regulations and cost, should a breach occur. The result is not limited to hefty fines per account breached, there could also be a loss of reputation which can result in much more severe consequences for a once-trusted business. If there are multiple offenses, it can lead to loss of license and prison time.

The average cost of a HIPAA-related record breach is about $200 per patient record and these costs are placed on the owner of the practice or organization. Most breaches will impact upwards of thousands of records. Any business must respond quickly if sensitive customer information is lost or stolen. Among other things, you may need to notify the affected customers and state and/or federal regulators.
Am I good to go if I do HIPAA training regularly and have patients sign the necessary forms?

The proliferation of Electronic Medical Records (EMR), coupled with recent breaches of patients’ personal health information and personally identifiable information, has highlighted the need for security of medical office networks.

Despite the EMR safety measures built into the 1996 Health Insurance Portability and Accountability Act (HIPAA), the element of human error and “it won’t happen to our practice” gets in the way of real security. HIPAA security rules require specific measures to ensure confidentiality, integrity, and security like passwords and PIN numbers to limit access to patient information to authorized individuals. Or encrypting stored information so that it cannot be read or understood except by someone who can “decrypt” it, using a special key made available only to authorized individuals. But this Act does not ensure a hospital system or single practice is safe from the ever-evolving threat landscape.
What can I do to help my healthcare business or organization increase security?

What was acceptable ten years ago as adequate security is simply not acceptable now. Network security line items should be added to IT budgets and should include a dedicated security team to monitor and protect systems.

Companies need to educate employees on security policies and should also be doing penetration testing multiple times per year by a security expert to try to break into your network to see if your security measures hold up. This includes not just technology, but physical access. Are your file cabinets locked and how do you open them? The more sensitive data that exists in your network or on your premises, the more frequently you should be doing penetration testing.

A crucial thing to consider is that people often think of network security as ‘firewall at the Internet,’ but just as important is securing the data that leaves your network. A business’s outbound policy is its last defense against a data breach.

Regarding data retention, there’s an adage in information security, “If you don’t need the data, destroy it.” So when companies determine they don’t have a purpose for personally identifiable information, they need an automated process, meaning no people involved, to delete that data.
Some industries have a good standard for getting rid of data. Take PCI DSS for example: if you don’t need that piece of data, there are specific guidelines that tell you to destroy it. In healthcare, HIPAA is more general or vague about how to handle data that’s not prescriptive.

Primary network ideals are to segment data based on its importance. Think about the payment systems in hospitals. The radiology department needs access to x-rays, imaging, and other diagnostic tests, but it doesn’t require access to a patient’s credit card information unless they’re sending out their own bills. Segmenting the network and using policies to limit access to only what’s necessary for a specific job function is critical.

So, what else can you do to protect your patients’ data and comply with regulations such as PCI DSS and HIPAA? Here are the most essential tips to help you stay ahead in the security game:
1. If you interact with credit card data and protected health information (PHI), you need to be HIPAA and/or PCI compliant; it's as simple as that.

2. If you accept any form of credit card, you will be required to be PCI compliant. PCI compliance levels are based on the number of transactions processed annually along with processing methods; this will dictate what level of compliance you require. Most merchants will be required to complete a self-assessment questionnaire, which is used to set a standard level of security.

3. Create a network segmentation security plan at your office/hospital that segments credit card information, patient data, security cameras, etc. Each segment should not be accessible by the others and should maintain a secure Wi-Fi connection.

4. Segment all departments/floors away from each other in order to create a modular network that if breached, attempts to contain the breach.

5. Lock down external-facing websites such as Facebook and Gmail. The weakest link in the security chain is, and will always be, humans.

6. Invest in high quality antivirus; do not be fooled by free versions. Spend the additional fees and implement a quality solution.

7. Add a UTM or NextGen firewall at the edge, married with a security information event management (SIEM) capability. This would immediately filter out most attacks, if not all.

There are also software solutions we would highly recommend. Most antivirus software works based on reputation and signatures, but there are certain solutions that block everything, unless they are specifically allowed. This type of software, the above list of tips, and end-user education would make such a system more of a hassle to breach than what it is worth; therefore, withstanding many of the modern attacks (including ransomware).

While this sounds simple enough, securing today's modern healthcare entity can be very expensive, and take time and resources to implement properly and continuously.
Tech Talk with Firewall Engineer, Felix Hernandez

This section details some of the major ways healthcare organizations and providers can thwart cyberattacks at every level and what it means to you.

First, we’ll start with the barrier between your local area network and the Internet. A network entirely behind a firewall is much less likely to be breached than one partially behind a firewall. This means, you should install your firewall directly between your modem and the rest of your network, with no other devices connected directly to the modem. This forces all traffic inbound and outbound from your modem to have to also pass through all of these wonderful virus and hacker stopping tools you have invested in. Fear not, NextGen firewalls can also perform routing and switching, so plugging the rest of your network into these will not stop your operations online.

A NEXTGEN FIREWALL has several software and hardware advancements that have pushed the known limits of what a traditional firewall is known for. NextGen firewalls in 2017 are equipped with so many different features designed to protect their networks that they have almost become a completely different device than the previous idea of what the firewall should be. Some of the more well-known features of these firewalls are: Categorization, IDS, IPS, Policy Management, Segmentation, and Virus Filtering. These features can and have been individually used to
dismantle an attack, but when paired into a single package, they become overwhelming for any attacker you have to contend with.

**CATEGORIZATION** is when a request is classified and then evaluated as to whether it is admitted or not. This level of protection is more useful in keeping employees from accessing known infected websites, or to contain viruses from spreading to entire networks, even from updating themselves. In many cases, this is the heart and soul of how a NextGen firewall becomes easy to use for anyone. These categories allow for blacklisting of content, not websites. This means that firewalls are now learning how to block or not block your request in such a way that offers the least amount of false positives and user frustration.

**INTRUSION DETECTION SYSTEM (IDS),** while being just three letters, is a world of hurt for hackers. IDS stands for “Intrusion Detection System” and is exactly as it sounds. This system analyzes inbound and outbound traffic for patterns which may be suspicious and logs them, followed by sending alerts. These systems are very effective against a large array of attacks because it identifies known attack patterns and gives the administrator crucial information necessary to mitigate such attacks from ever happening again in the future.

**INTRUSION PREVENTION SYSTEM (IPS),** while being similar to IDS, is another feature or tool in the arsenal of a NextGen firewall. In most cases, vendors are now including both of these features in a single unit. This is because where an IDS monitors traffic, an IPS controls traffic. In an ideal configuration, both of these features can work side-by-side and even complement each other. An IPS evaluates inbound and outbound traffic and denies any such traffic that it finds to be dangerous.

**POLICY MANAGEMENT** is the proverbial shield of a NextGen firewall. Even in more traditional firewalls, this was the tool that made them the anti-hacker tool of choice for many large corporations and governments. The theory behind this tool is that the less you allow, the less the hackers have to work with in order to breach your network. Think of a policy as a set of rules that you give the firewall in advance. Everything that follows your rules enters, but whatever doesn’t follow your rules gets blocked. Over the years, policies have become more and more complex.
Policy management is now to a point in which you really want a trained professional to establish these rules so that they may be fine-tuned toward the least amount of false positives, but highest amount of protection.

**SEGMENTATION**, the new kid on the block, is as powerful as every other asset/tool in the NextGen firewall’s arsenal. It is important to mention, segmentation is not something new at all, but has begun to see a rise in popularity over the course of the last few years. The theory behind segmentation is that the less surface area of your network you allow any attacker to touch, the less likely they are to fully breach your network. There is an absolute need for such a tool as this would ultimately separate different computers into completely different networks which can’t communicate with each other. This feature not only assists with protection networks, but also helps keep networking costs down.

All systems that handle sensitive customer data should be segmented into their own private network, which other networks cannot reach. This kind of network is often called a “Trust” network, derived from the idea that we trust this network with sensitive information. This means, if you have any points of sale, or databases holding customer information, the “Trust” is where they should be. Any other system that requires Internet connectivity, but is not holding sensitive information, should be within its own network or networks. This is so that if any of these non-sensitive systems becomes infected, the infection does not spread to the credit card terminals or customer databases.

**VIRUS SCANNING CAPABILITIES** are seen in most NextGen firewalls. Some can even scan incoming emails. This additional scan assists with protection against all sorts of malware, possible phishing, and even spam blocking. Remember, this should never be a replacement for a traditionally known and reputable virus scanner on every computer within your network. These scanning capabilities are merely a preliminary scan, and do not completely remove all possibility of malware-infecting systems. There are many reputable options of antiviruses; Avast, BitDefender, Kaspersky, McAfee, Norton, and Webroot to name a few. Do your research as to which one would best suit your needs.
SECURITY INFORMATION EVENT MANAGEMENT (SIEM) systems are almost crucial to a secure network. SIEM systems are a combination of Security Information Management (SIM) systems and Security Event Management (SEM) systems. These systems allow Information Security professionals to manage and record attacks on your network. These systems can even be used to prevent future attacks on your networks, with their ability to monitor and record even the most minor events!

PATCHING is imperative for computers and programs. If you are not keeping up with regular patching of your computers and the programs that run on it – then you are simply asking for trouble. Many of the breaches that make the news (and I am sure many more that don’t make headlines) are caused by holes in software for which a patch existed by the vendor. What you want to avoid is the delay of patches from getting applied. It is ok to postpone the application of patches until later in your day or when you shut down the computer. But, you should never delay more than needed and I would say it is never advised to go more than 48 hours after the patches are available to get them applied. Keep in mind that a compromised system may hurt not only that one system, but others as well. If you use your computer on a network that includes other computers, your issue could affect them too.
CONTINUOUS END-USER EDUCATION is a vital key to network defense. There are many thousands, if not millions of dangers on the Internet, and many more being discovered daily. Think of these new threats like an animal; they don’t bite until they do, and then they bite. In other words, many threat prevention tools will not consider them a threat until they become one and then they are a threat. This means that even a computer system running every other security precaution can be breached easily with a new threat, when the computer user makes one wrong move. For starters, never open attachments or links from a source that you do not know. Never use a system within the “Trust” network to perform tasks that can be performed on another system outside of that network. Never set simple passwords that are easy to guess and always use different passwords on different websites/services.

SYSTEM UPDATES are the last recommendation but not the least important! Keeping up-to-date is as important as having a properly configured firewall on your network. As of April 2016, there was a study that showed there are still millions of computers running Windows 7 and older. These systems are easy prey to viruses and malware which was made specifically to plague these systems and even automatically spread to more systems like them. Along with the massive virus issues plaguing these older systems, there are also several known vulnerabilities in these systems’ core programming. The frightening part is that since these systems have been around so long, the hackers have had ample time to really test, create, and implement all sorts of tools to wreak havoc on any network containing these outdated systems. Keeping up-to-date does not necessarily stop hackers and viruses from affecting you, but it definitely makes their job much harder by giving them less and less time to come up with ways in which they can attack you and your network.

Any network following these guidelines could help make itself intolerable to any attacker, and exceedingly difficult to attack, due to the constant frustration of not being able to even penetrate simple systems. The only effective way to fight off hackers is to limit any attempts they make to gain information, and constantly have systems updating so that when they do gain the information they need, your system environment has already changed and their information is void. Regular security scans or penetration testing and auditing are the only reliable way in which you can know that these principles are reliably being followed.
In Summary

Whether it’s a hospital system with multi-location brands, an urgent care facility, or a doctor, chiropractor, or dentist with a single practice, the computer network in those offices can quickly become highly complex, exponentially increasing the risk of data theft. A single breach can cost millions. At stake are not just the mitigation costs, but also the potential for lost trust and confidence, and court-ordered compensation. Netsurion remotely manages network security and assists in both PCI DSS and HIPAA compliance for healthcare organizations that require a safe and secure network.

While it is impossible to say that a system can never be breached, if you are not doing some of the basics to help protect your system and your data, then you are more likely to experience a breach. Healthcare entities are more prone than other types of businesses to attacks, simply due to the fact that they handle many types of very sensitive data, including employee data, payroll data, insurance data, and patient medical related data. And don't forget about payment related data, which has its own set of protection requirements and regulations.

A good security plan can be overwhelming at first, but with the right knowledge and expertise, it can be simplified and managed to reduce the exposure of your practice or hospital and limit the amount of risk. No matter how small your organization is, you should still stand up against the hackers. Don’t let them come in and win the game. No security plan is foolproof, but ignoring compliance standards and security needs is a risk you don’t want to take.
About Us

Netsurion powers secure and agile networks for highly distributed and small-to-medium enterprises and the IT providers that serve them. In such environments, the convergence of threat protection and network management are driving the need for greater interoperability between the NOC (network operations center) and the SOC (security operations center) as well as solutions that fuse technology and service to achieve optimal results. To this end, Netsurion has converged purpose-built network hardware, innovative security software, and flexible managed services.

Netsurion’s SD-Branch solution, BranchSDO, is a comprehensive network management and security solution consisting of SD-WAN, next-gen security, cellular, Wi-Fi, and PCI DSS compliance tools and support. At the heart of the solution is the CXD, Netsurion’s SD-WAN edge appliance.

Netsurion’s Security Operations solution, EventTracker, delivers advanced threat protection and compliance benefits in a variety of deployment options: a SIEM platform, a co-managed SIEM service with 24/7 SOC, and a managed SIEM for MSPs.

2017 CYBERSECURITY EXCELLENCE AWARD WINNERS
Netsurion: MANAGED SECURITY SERVICE
EventTracker: SIEM