Cyber Security Services

A Necessary Evolution in Healthcare Security

Evolving from "Protect, Detect, and Respond" to a model that helps prevent attacks and reduces risk exposure, understands the threat landscape, proactively sees vulnerabilities before they emerge into exploits, and moves the focus beyond the perimeter to the approaching enemy.

Authors:
Darian Lewis, Sr. Principal Threat Analyst, Symantec CSS
Eric Gonzalez, Principal Threat Analyst, Symantec CSS
Nicholas Zulkoski, Sr. Threat Analyst, Symantec CSS
Contributors:
Axel Wirth, Distinguished Technical Architect, Symantec TSS ES
Maria Swainson, Director, Symantec CSS

21369616

Contents

The Old Guard

Detect, Protect & Respond

It has long been held that the correct approach to cyber security is to protect the network borders, watch out for attackers approaching and crossing the border, respond accordingly and recover as quickly as possible. As recently as 2010, this was a generally accepted best practice and given as the right approach and good security advice (Microsoft, 2010). Five to 10 years ago it may have been the best advice you could receive.

However, times have changed as have your adversaries, their goals, the approaches they take, their speed of action and the resources they have available. Additionally, healthcare has a more complex digital infrastructure containing more valuable data and a less well-defined perimeter with mobile devices and cloud connectivity providing additional routes for data movement. Your adversaries fully understand the value of the data they are after and develop a well-crafted and targeted attack to reach their goal. Gone are the days of the glory hacker getting his or her name into the limelight, or the get-rich-quick hackers. They may still exist, but they are dwarfed in number by cyber terrorists, hackers with political agendas, corporate and government-funded espionage attackers, well-funded cybercrime gangs, and a host of other malicious actors.

It is time to evolve from “Protect, Detect and Respond” to models that actually help prevent attacks and reduce risk exposure, understand the threat landscape, proactively see vulnerabilities before they emerge into exploits and move the focus beyond the perimeter to the approaching enemy.

Laws protecting consumers such as the Privacy Act of 1974, Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act) are the tools being used by the government to enforce protection of consumer healthcare data. HIPAA was introduced to help prevent either accidental or intentional disclosure of Protected Health Information (PHI). PHI includes names, addresses, dates of birth, social security numbers, diagnosis codes (ICD-9/10), medical billing codes and other identification numbers.

HIPAA originally did not have serious “teeth” in that the fines were relatively low – ranging from $100 to a maximum of $25,000 – nor was it seriously enforced (Mohammed, 2015). The HITECH Act of 2009 changed that, namely making fines tiered depending on culpability. Where neglect is involved, fines are increased up to $50,000 USD per violation with a maximum cap of $1,500,000 USD per year for the same kind of violation, in the same year. Also, HITECH mandated that Health and Human Services (HHS) instate HIPAA audits as well as introduced the obligation to report breaches over 500 records within 60 days of discovery.

In 2013, these cumulative changes where consolidated in the HIPAA Omnibus rule, raising the bar on patient privacy and making these new requirements, including breach notification mandate, tiered liability and higher fines, the law of the land.

Even though the fines for HIPAA violations are increasing, what we have learned over time is that civil penalties aren’t persuasive enough to encourage security, either because the fines aren’t high enough or because it is still easier to cut costs on security and simply take the risk (Mohammed, 2015). Cyber security insurance is the new

fallback plan. It can address residual risk issues and provide some security for many but for some, it may be a crutch to lean on while delaying more appropriate security controls. HIPAA also is not very prescriptive. It tells you what you should accomplish, but not how those goals should be implemented.

Many organizations are having financial challenges and security is often viewed as an investment with no direct payback and obvious benefit. If there's no choice due to audits, healthcare organizations have been seen to do the minimal required to pass the audit, in the least expensive manner possible – in a way taking a checklist approach to compliance and security. The end result is insufficient security which leads to the conclusion that compliance is also an ineffective way to promote and ensure information security.

A Firewall Is All I Need

There may have been a time when a firewall was all an organization felt was needed to be secure. At that time, anti-virus software was the epitome of endpoint protection. All employees were perfectly loyal and the thought of insider threats was unimaginable. That world never really existed, but some people believe that it did.

Techniques for getting through firewalls, called "FireWalking", have existed for some time. There are even tools, such as *Firewalk* available through nmap.org, that allow attackers to use TTL values and ICMP packets to discover the access control list (ACL) filters to evade them. This is just the first part of an attack – active reconnaissance.

Firewalls are just one example for what can be considered a fundamental lack of understanding of today's security. Weak passwords are still used, little-to-no use of two-factor authentication, lack of review of system access, no audit policies, and no regular security assessments are only a few of the problems in healthcare security. The result is hackers gaining access to PHI more easily and a reactive posture, rather than a proactive one as it relates to information security (Mohammed, 2015).

The Necessity of Reading Logs

IT staff is difficult to find and hire. Security staff is in high demand due to a massive upswing in cybercrime, making these resources even harder to find and retain. Furthermore, like many other industries, healthcare isn't easily finding the funds to hire more IT or security staff. Yet, many do not have the ability to dedicate their staff's time to analyzing the security and event logs. Nevertheless, end point terminals and devices, network monitoring equipment, security gateways and other products continue to generate an ever-increasing volume of information. The subtle indications of external probing are in those logs and if they aren't carefully examined continually, the attack you weren't expecting will happen and data will begin flowing out – and keep flowing out unseen. Using a managed, external service like Symantec's MSS to complement in-house talent can free up these highly-valued and difficult-to-obtain resources, while allowing continuous monitoring and alerts on indications of threat and compromise so you can act quickly. For more information on this Symantec offering, visit https://www.symantec.com/services/cyber-security-services/managed-security-services.

Hackers have a sophisticated arsenal of tools to use but actually haven't had to deploy many of them because very simple and older techniques continue to be effective against

healthcare organizations. Yet at the same time, the interest in health data is increasing because of their high monetary value in the underground market, as well as their broad application to a variety of uses. (Vogel, 2012).

Damages

As part of the care delivery process, patients share information with their care providers, and health IT systems amass more and more information. Admittedly, patients also submit large volumes of healthcare-related information to public websites, but the information they turn over to healthcare providers is entrusted to those organizations. Under HIPAA and state laws, these organizations have an obligation to protect personal patient information from accidental or intentional disclosure.

Yet, across all industries, the healthcare industry has the longest security event duration and time to detection for a compromise (Moore, 2014).

A New Way to See the World

There are two complementary models in threat intelligence that are currently used: *The Cyber Kill Chain*™ and the Diamond Model. These models are used to describe threat actors and the attacks they perform against other entities. Most security tools today use these models and concepts to track threats, threat actors, and other security concerns and events.

The Cyber Kill Chain™

The Cyber Kill Chain™ is a model developed by employees of the Lockheed Martin Corporation to address and describe the more advanced threat actors they describe as Advanced Persistent Threats (APT). The name and the concept are similar to the military usage of kill chain. In the military parlance, the kill chain describes the steps or phases of the campaign from target identification through destruction of the target. Lockheed Martin extended this concept to the cyber domain to explain an attack by threat actors.

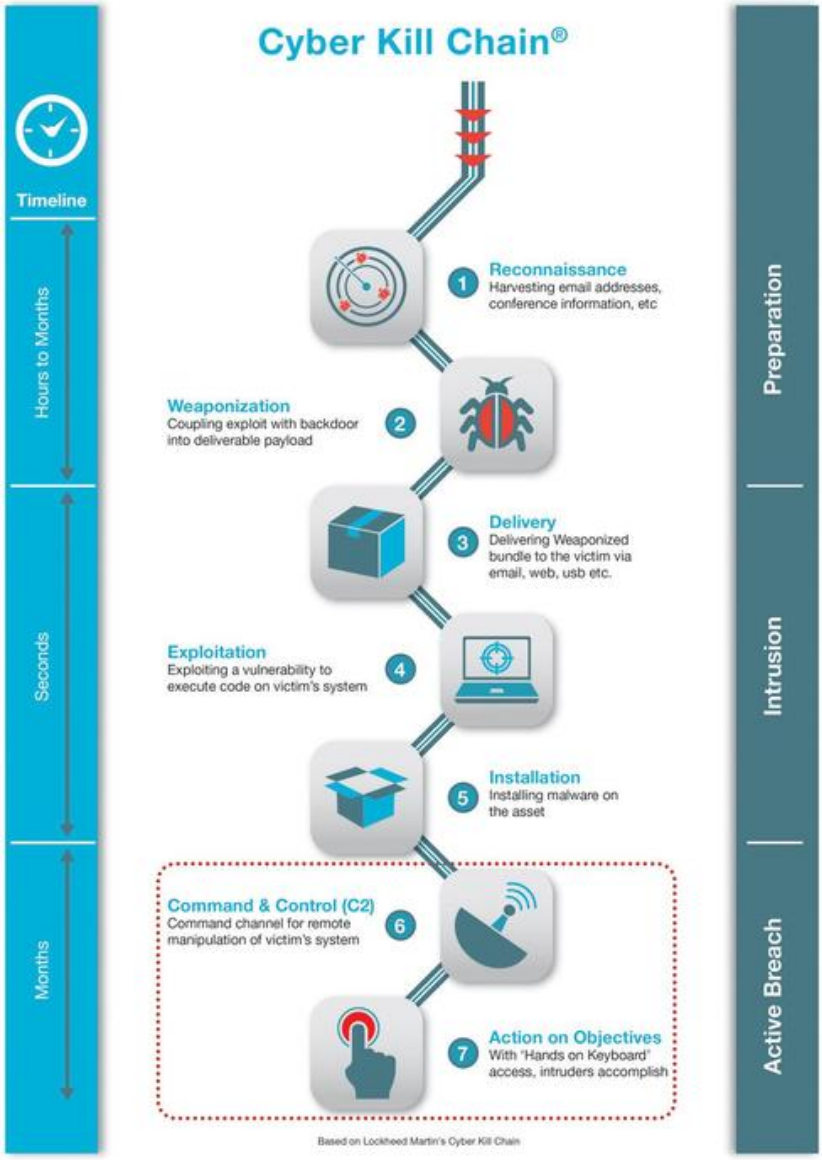

Figure 1: The Cyber Kill Chain™

The Diamond Model

The Diamond Model was created around 2006 to address concerns in characterization of threats, ability to track evolving threats, differentiation of threats and the counteraction of threats. The model is based both on theory and practical experience. Its origins are in graph theory, and the model provides both fundamental concepts for new ontologies as well as the backbone for many security products on the market today.

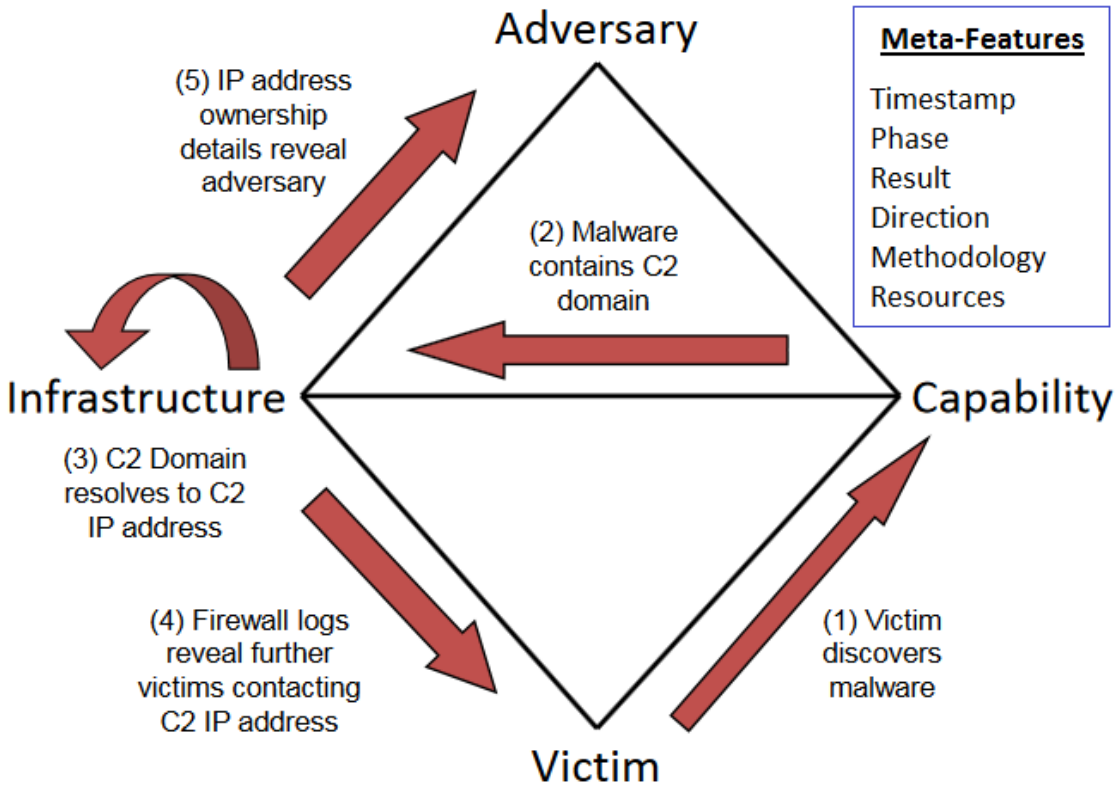

Figure 2: The Diamond Model

The model is based on a security event, represented as a square sitting on one vertex of a diamond. Each vertex represents a characteristic of an event: the adversary, the infrastructure owned or used by the adversary, the capabilities of the adversary and the victim. There is also metadata about each of event including time, phase in the Kill Chain, the result of the incident, the directionality, the methodology of attack, resources used for the attack, etc. This model is frequently used to pivot between various diamonds during the aforementioned kill chain phases. This allows users to graphically represent attacks and uncover information that would otherwise be difficult to see.

Intrusion analysis

If the worst case scenario happens, and criminals do gain access to your infrastructure, the best possible outcome is through quick detection and remediation. To be able to see the attack, your organization has to continually read logs and analyze them for unusual patterns. That can present a strain on resources as each device adds a tremendous additional workload. Automated tools to aggregate and correlate incidents can only tell you something is odd about a group of incidents but usually can't describe why or what the exact threat is. That requires highly skilled talent. If you don't have it in-house, you should consider outsourcing it to a managed security services provider (MSSP).

Campaigns

In the cyber threat landscape, healthcare represents the proving ground for a myriad of techniques. Criminals are making use of trojans, backdoors, zero-days, and any attack vector they can think of to achieve their goals. The reason is that many healthcare organizations provide a soft target -- all of these different approaches have been proven to work. That is not to suggest attacks against healthcare are simple and easy to avoid,

quite the opposite. As the value of healthcare records continue to rise, up to $50.00 USD per record on the black market by some estimates, cyber-attacks grow more complex (Rashid 2015). A *Cyber Kill Chain*™ analysis of these attacks speaks to this idea of increasing sophistication.

In the early stages of a typical healthcare attack, attackers have proven their flexibility and capability. Healthcare in particular demonstrates the success rate for many forms of reconnaissance beyond typical port and network scans. The *Institute for Critical Infrastructure Technology* notes the capability of social engineering in the modern threat landscape. Phishing emails carrying malicious payloads are a particularly effective method of initial infection. In many cases attackers will even bolster the legitimacy of the message using convincing information stolen from previous campaigns. Operations incorporating this methodology have proven hugely successful; as the ICIT puts it "employees are culturally programmed to open emails and because attackers obfuscate the insincerity of the message."

Moving right along the Kill Chain, we continue to see a variety of tactics. Specifically, healthcare targets have fallen victim to both the "fast and hard" and "low and slow" approaches to data exfiltration. "Fast and hard" in this case describes an operation that values speed over stealth. This can involve zero-day vulnerabilities, loud malware that lacks obfuscation techniques, or even simply a stolen laptop. This may seem like an unsophisticated and cumbersome technique, but *Forbes* notes in their 2015 Healthcare Retrospective that a stolen laptop has led to a data compromise of 160,000 records (Munro 2015). Alternatively, "low and slow" describes the type of data breaches that dominate the news - the use of hidden backdoors, obfuscated malware, or falsified personas within the network. In 2015, the average time it took to discover a breach was 205 days. In that time, a huge number of records could have been exfiltrated and the network entirely compromised.

Lately the trend of attacks against healthcare organizations has been to use ransomware -- a relatively new type of malware that encrypts the files of the victim computer. If an employee does open an attachment or run a program attached to an email, nothing may appear to happen immediately. Within an hour to a day, the computer will begin to show messages that indicate your computer is now being held hostage and that you will have to pay to get your data back.

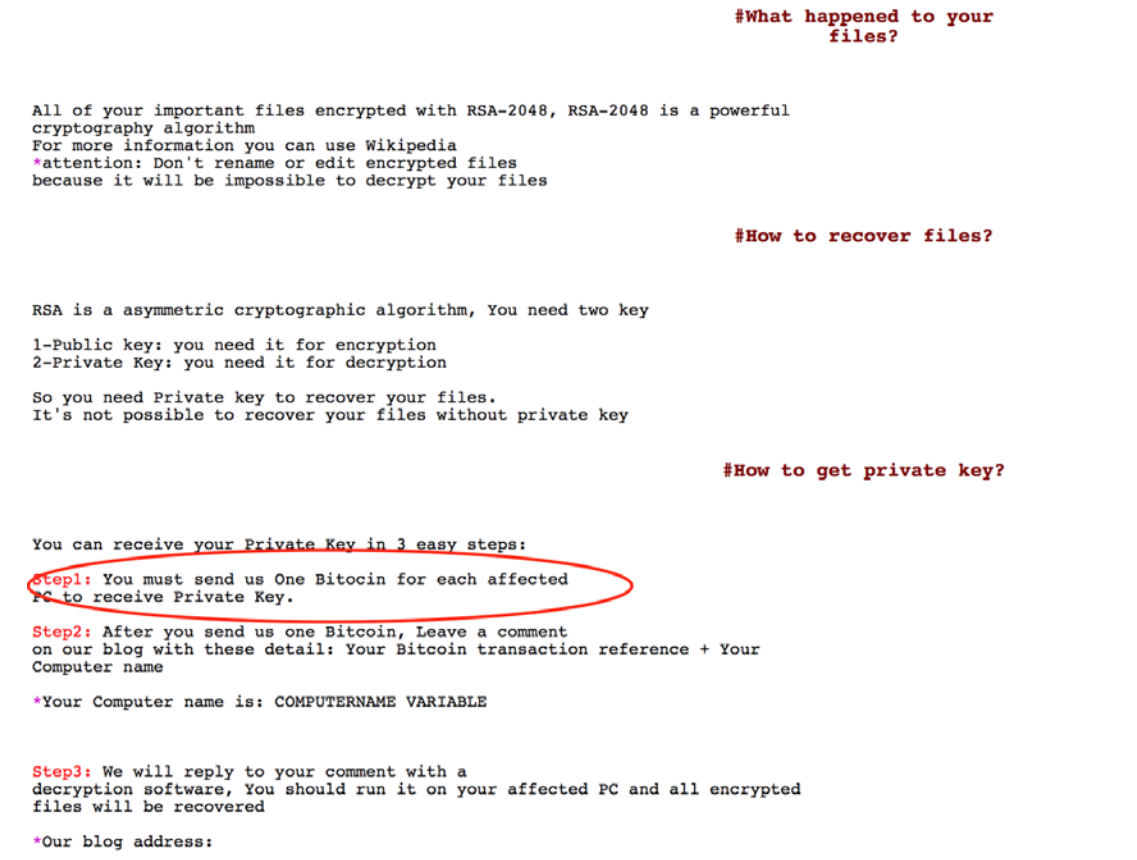

Figure 3: Ransomware message shown to infected computer users

Like most malware, the initial delivery vector is usually email, typically phishing or spear phishing.

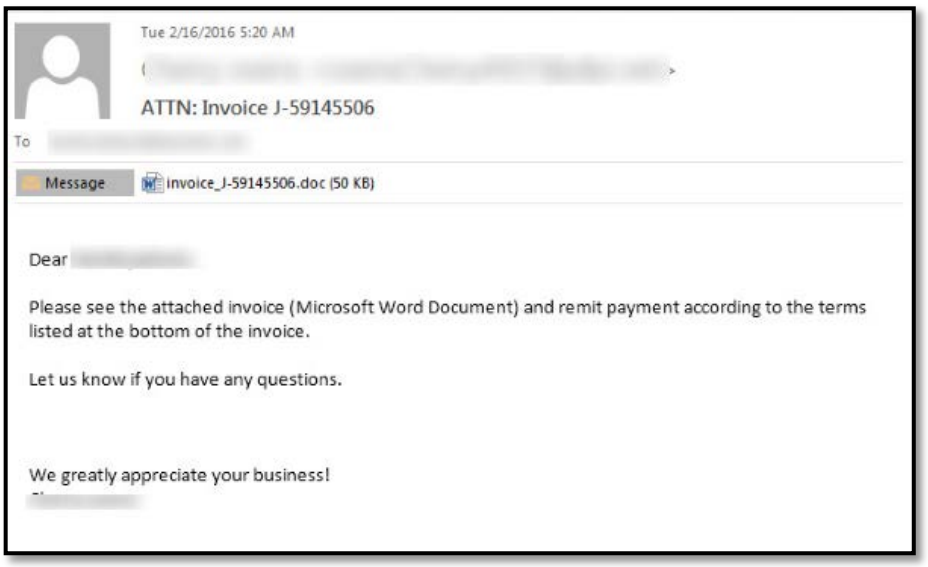

Figure 4: Phishing email leading to Locky

The example phishing email in Figure 4 shows an example of a “Locky” delivering email. Locky has been used with increasing frequency against healthcare and related organizations. You may have seen the outcome of these attacks in the news where hospitals and medical centers have had to completely shut down all of their desktop computers and web-based systems to keep the Locky malware from spreading. It is not yet viral in nature, spreading computer to computer with its own malicious code. However, once Locky infects a file in a shared folder, other employees opening the file also become infected and it can quickly spread across departments and the entire organization.

These are the steps you should take if you become infected with ransomware:

1. Activate your Incident Response system immediately. If you don’t have an Incident Response team, Symantec has you covered. Call **855-378-0073** to immediately begin the triage process. You can read more about Symantec Incident Response at https://www.symantec.com/services/cyber-security-services/incident-response
2. Contact law enforcement and your legal counsel for advice.
3. DO NOT PAY THE RANSOM.

The last point is maybe the hardest thing to hear when you’re in the midst of a crisis, but it is the best advice you can receive. Even though the criminals may tell you they are going to double the ransom every day, don’t pay it.

Paying the ransom only feeds the system and encourages the criminals to continue. Second, they may not unlock your files or may leave a good deal of malware behind for another attack later. Third, even if you pay, and you get your files back, you’re on the list of people who will pay, and you are at risk of being hit again (and again..).

The best reason not to pay, however, is because you should have a full backup and restore system in place as part of your compliance requirements. You may lose some data back to your last backup, but you can recover and the resources above will help you get back to normal operations as safely and quickly as possible.

“Run the Business” Mitigation vs. Strategic Mitigation

Many organizations attempt to implement the fewest possible security countermeasures that meet regulatory requirements and keep the business running. Criminals are counting on that behavior as it makes their work much easier to successfully complete. Looking further left on the kill chain to find criminals that target your organization and learn their techniques, tactics, and procedures (TTPs) will allow you to block them earlier in the cycle. By performing this activity you will be able to prevent many of the ultimately damaging and costly attacks that are occurring daily.

The costs of a single Locky infection range from a few Bitcoins (a relatively untraceable crypto-currency) to hundreds of Bitcoins to recover data. In case you are not familiar with Bitcoins, their current value is approximately $450.00 USD each. That may not seem like much, but medical centers have paid tens of thousands of dollars to try and get their data back, only to fall prey to the same attack a short time later. Additionally, you have the cost of incident response, lost revenue and impact to your reputation.

Moving "Left"

A good security strategy and a well-prepared organization can spot an attack in progress, but a great one can prevent it all together. The goal of cyber threat intelligence is to guide individuals or groups left down the Cyber Kill Chain from mitigation to anticipation. This can be accomplished using the following methods:

Know thyself: Understanding your organization's assets is critically important in identifying and mitigating threats. Take an inventory of valuable information - including patient health data, insurance numbers, user credentials, business information or in-house research. The nuances of this data defines your placement within the healthcare landscape. Be mindful of ongoing campaigns and use your newly defined placement to understand their relevance to you and the risk to your organization. Combat the specific TTPs used in said campaigns with specific mitigation strategies. Suddenly, what was a chaotic barrage of nefarious activity becomes a calculated intrusion with apparent directionality. Storage devices known to house this newly "critical asset" become monitored more closely and a sensible, thought-out defense architecture becomes apparent. When it comes to justifying a security budget, this point could not be more crucial.

Know thine enemy: A critical incident does not exist in a vacuum. Behind each cyber-attack, there is a story of why it occurred, what specifically happened, and most notably, who did it. Threat actors can be complex entities -- they have a command structure, constituents to report to, and a human element that is often unappreciated. Most importantly, they are human beings who make human decisions. Research what threat actors exist in your space and understand the tools, techniques, and practices they use. Then, design a defense strategy that counteracts or prevents these attack methodologies. Ensure this defense strategy is comprised of both human and technical elements. Instruct employees on proper conduct in the face of suspicious emails, implement a security protocol to account for specific TTPs threat actors used in your market vertical, and research what technology fits the situation best.

A thousand battles, a thousand victories: Security preparedness is a skill that needs to be learned and practiced. Cultivating a culture of knowledge is key to building a strong defense. Industry roundtables, tabletop exercises, and an ongoing dialogue about policy and techniques are all key to promoting an informed security posture. For many healthcare organizations, the experiences and opinions of peers represent a vast, untapped resource. Cooperation between targets is simply something cyber criminals do not account for. If your organization finds itself as the target of a cyber-attack, share live malware samples within the threat community, warn others when a campaign is in action, and practice transparency about the nature of the attack. Industry roundtables provide an excellent opportunity to accomplish these tasks.

Protecting Assets

What Are Your Assets and what are they worth to you?

Any networked or otherwise interconnected asset is a possible target. Most healthcare industry attacks are centered on stealing patient data. But as fallout from an attack, systems can be shut down or made unusable. In the recent case of a Los Angeles hospital, access to the systems themselves was withheld, as the access itself was an

additional monetization factor in the attack. Other attacks since have led hospitals to go back to operating with paper while the damage from an attack was being repaired.

Any asset is a possible target, and the goal of criminals in attacking healthcare organizations is to monetize the information they steal (Johnson, 2016).

Databases

Safeguarding electronically Protected Health Information (PHI) and the databases that house them is a HIPAA requirement. The black market monetary value of PHI data is the reason healthcare organizations are targeted by attackers.

Although the database itself should be strongly secured against direct attacks, multiple systems provide access to patient records, from traditional desktops to mobile devices. So any system that accesses medical information from a database is a possible target; it can serve as a pivot point for attackers to access the database directly. If data can be secured in different databases, on different servers, damage due to a database exposure can be limited.

Devices

Security patches for known vulnerabilities can't easily be applied to medical equipment. There are regulations in place to prevent any changes from being made without approval from the manufacturer. Deploying upgrades or patches to medical devices without coordination with the manufacturer will likely result in the equipment losing its FDA certification (http://www.fda.gov/MedicalDevices/). Because of the poor device security posture coupled with the care or even life-critical functions they provide, these devices should be kept as isolated on the network as possible and should be protected by additional mitigating controls like firewalls and security gateways.

Networks

To accommodate the modern age, hospitals and clinics offer Wi-Fi access to patients and guests, expecting network segmentation would be sufficient. Most organizations are unaware that attackers can locate and utilize Wi-Fi access points as pivot points to the rest of the network. This is due to improper network isolation, as these networks are often open with little to no security in place.

Network isolation should be done at every layer possible and if direct Internet access isn't required, an asset should be protected as an internal network asset with only the network access required for operation. It is particularly true of medical devices that may have vulnerabilities and typically are behind in patching or may even run an end-of-support (EOS) operating system.

Software

Many systems used in hospitals and clinics are legacy systems with new applications built on them. This leaves unresolved vulnerabilities in place. Many medical systems have a long useful life and, in spite of running on an outdated platform, still perform a useful clinical function. There is very little value seen in updating/upgrading these systems that have been operating flawlessly for years. From a clinical perspective, there is little concern about continuing to use the platforms. Unfortunately, these platforms are

a significant security risk. Often there are additional dependencies on these systems that prevent an upgrade without causing a cascade of upgrade requirements. This can quickly become a more expensive problem to solve.

In light of economic realities and the often slim profit margins in healthcare, it is a challenge for most healthcare institutions to allocate the funds required to maintain a state-of-the-art IT infrastructure.

Customer Data

As previously discussed, Protected Health Information (PHI) is easily monetized by attackers who obtain it. In addition to any financial penalties incurred for HIPAA violations, brand image and customer trust may get compromised. Brand value is one of the most contested topics in business. For healthcare providers, it is an intangible asset that can be the reason a physician makes a referral, or a patient chooses a provider. According to the Ponemon Institute, a data breach of a healthcare facility is the most expensive breach to remediate. The average cost of a data breach for healthcare organizations worldwide is $363.00 USD per personally identifiable record exposed. IBM conducted a separate study and found a similar result at $398.00 USD per personally identifiable record lost. (http://www.modernhealthcare.com/article/20150528/NEWS/150529899).

Australia has a universal healthcare system called Medicare. The Medicare Card Number serves as a unique identifier for every Australian resident, including a tax file number. A Medicare card can provide anyone a wide extensive medical service for free or highly discounted/subsidized. Regardless of whether the medical system is universal healthcare-based or for-profit, the threats to healthcare providers and associated organizations continue to increase. Many other countries have a similar system of nationwide insurance identifiers as well, including the U.S.' for-profit system which uses social security numbers as identifiers far too often.

A concern highlighted by one of our healthcare customers is that all medical services require Medicare, and therefore the Medicare card number. Everyone's health record in Australia is tied to a Medicare number and this record is stored in one centralized system. A single breach on this system could reveal the entire nation's medical records.

This further emphasizes the need to keep medical and service data separate and isolated. A single Medicare number in Australia is similar to the social security number in the U.S. and identity numbers in other countries. Essentially, these numbers tie all records together easily – both for healthcare providers and for criminals. That is why medical records are so complete and therefore fetch a high price on the underground markets.

What Should Be Done?

The breach of the Veteran's Administration (VA) demonstrated the non-existence of even the most basic security controls (Mohammed, 2015). Security needs to become part of the healthcare provider corporate culture. In an industry that has been described as "plagued by perpetual attacks from numerous malicious hackers" (ICIT 2016), security needs to be a primary concern. Not only that, but it needs to be a part of its

business objectives as well as budget. In October 2015, Healthcare Informatics ran a survey of security workers in healthcare organizations and found that half said that 10% or less of their overall IT budget went towards cyber security (Leventhal, 2015). A study by Symantec partnering with HIMSS showed that top-level leadership has a lack of urgency and understanding of security as a business issue rather than just an IT issue. (Symantec and HIMSS, 2015) A realistic approach needs to be taken to building a working security program, and this requires funding as much as it does understanding. Fundamentally, the perspective needs to change.

Healthcare Threat Landscape

The number of criminal cyber-attacks on healthcare organizations is increasing dramatically. This is due to the value of the stolen data on the dark web and in black markets. The Ponemon Institute has reported that 90% of health institutions have reported experiencing a cyber-attack since 2012. (Mohammed, 2015)

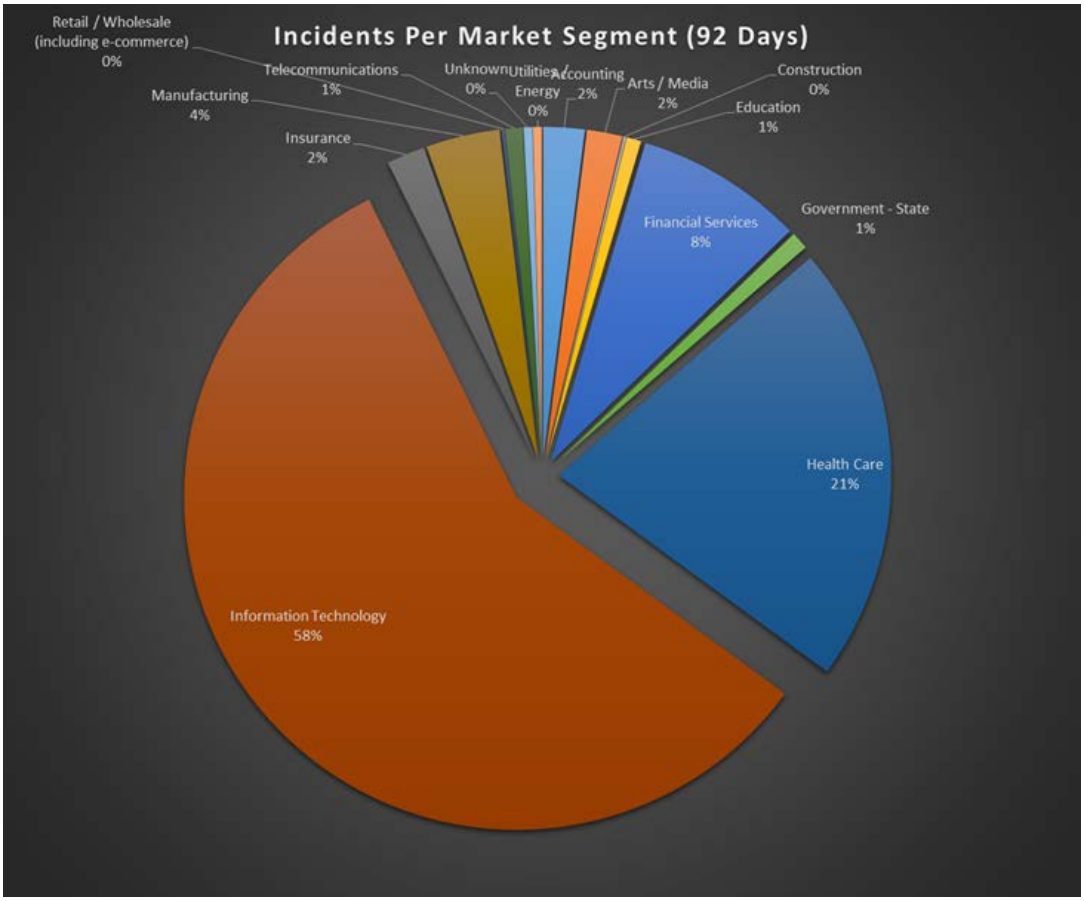

Figure 5: Attacks Seen by Symantec, Organized by Market Vertical

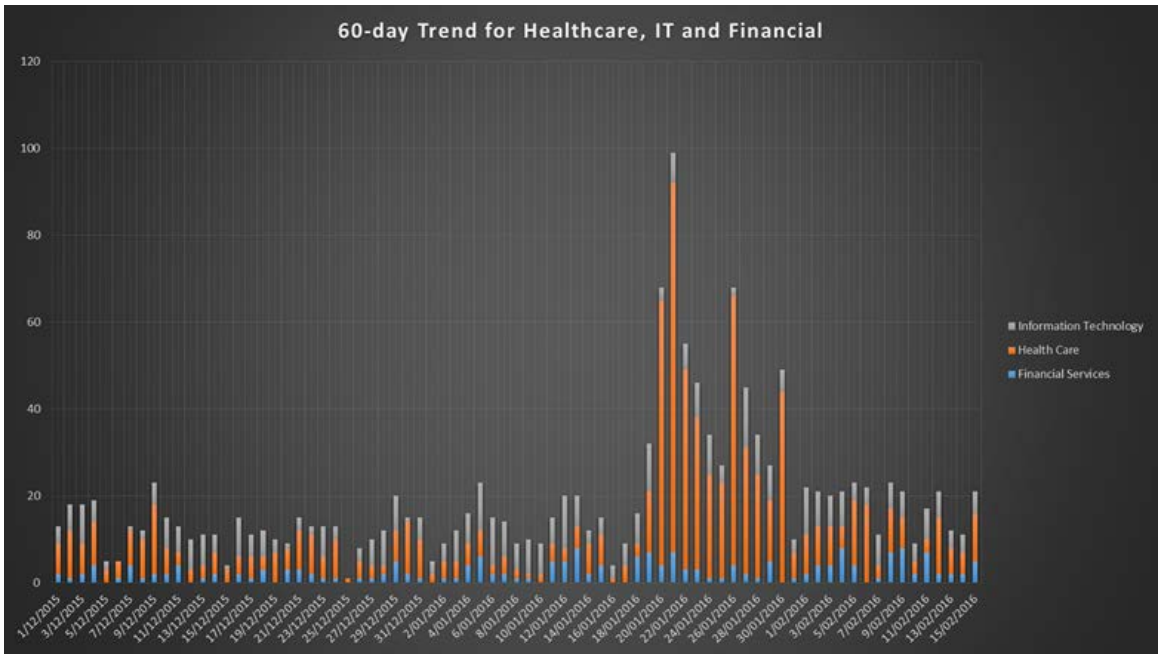

Figure 6: 60-day Trend for Attacks Against Healthcare, IT, and Financial Organizations

Lately, Qakbot has been used extensively against healthcare organizations. Qakbot has had an unusual effect on Windows XP systems, which caused them to crash. Recovering from this attack has been very taxing for healthcare organizations. Given that many pieces of medical equipment are still using Windows XP-based systems, the damage that can be done by this malware alone is evident.

The most recent and disruptive attack against healthcare organizations in 2015 and 2016, though, has been ransomware.

Ransomware

What is Ransomware?

Ransomware is malicious software that disables some functionality on a compromised system (O'Gorman & McDonald, 2012). There are two types of ransomware: locker ransomware and crypto-ransomware. Of the two, crypto-ransomware is being used the most against healthcare organizations due to its effectiveness in eliciting a user's response to pay the ransom.

Ransomware has quickly become one of the most dangerous and prevalent threats facing organizations today. This holds true in the healthcare industry, where multiple organizations have had sensitive information held at ransom by attackers.

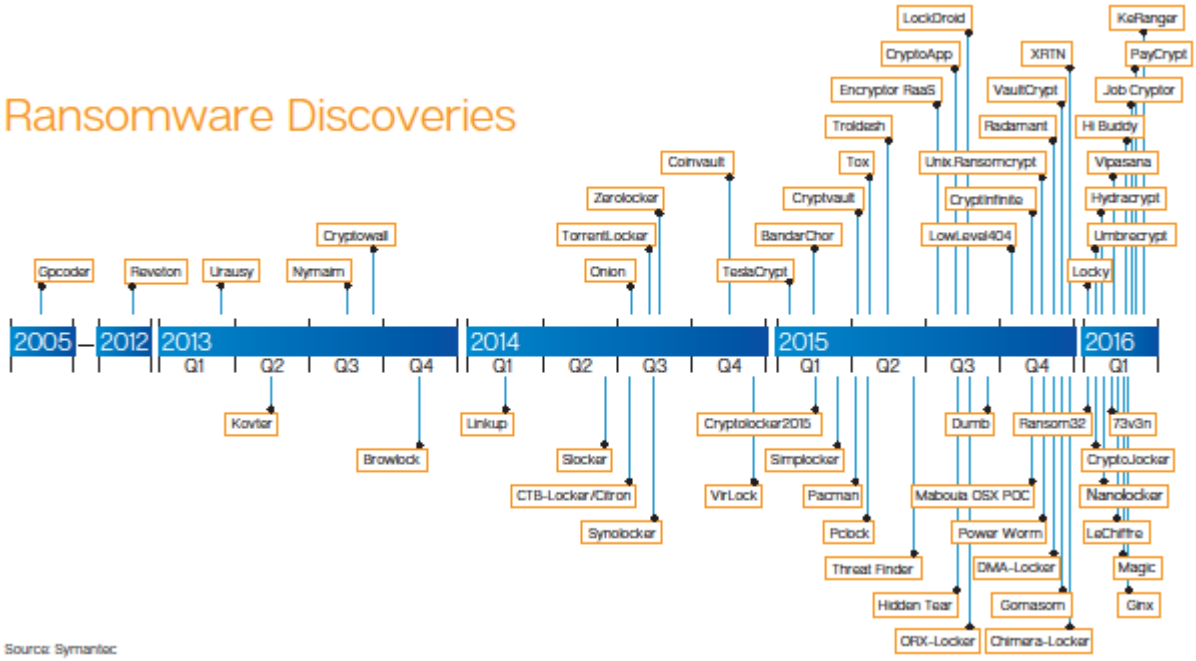

Figure 7: Ransomware Discovery Timeline

The figure above demonstrates the increased focus by attackers on creating new ransomware variants. Last year sparked the increase in the observance of new ransomware variants while 2016 shows it trending towards higher discoveries being made.

Cases like the “Medijack hack”, where hospital equipment was compromised, proves that the use of ransomware via an already breached network is very likely (Paganini, 2015). In September 2015, we observed another case where a hacker that goes by the handle “x999xxx”, attempted to sell access to a compromised network on a hacker forum. No interest was garnered on the forum so the hacker resorted to deploying ransomware on the compromised host in attempt to collect money via another avenue.

Ransomware attacks have been increasing in frequency against healthcare organizations. The impact on affected organizations has been devastating. A Kentucky hospital shut down its external web interfaces and put up a warning they were in the midst of a crisis. A Washington, D.C. healthcare organization completely stopped using electronic records and went back to using paper while their crisis was being handled.

Healthcare Best Practices for Ransomware Threats

Symantec wants to be your trusted advisor and with the recent attacks of ransomware against healthcare organizations, now more than ever that advice can help you avoid becoming a victim.

First and foremost: **DO NOT PAY THE RANSOM**. There are a number of reasons not to pay; your data is essentially gone at that point. Paying any money doesn’t guarantee you’ll get a byte of it back – there is no honor among thieves. Paying the ransom will

absolutely make you (and in a sense the larger industry) a target for future attacks because you paid. Finally, you are essentially validating a criminal economic system that then funds even more complicated crypto malware. Criminals go where the money is. There is an excellent Symantec thought leadership article written over a year ago by Matt Sherman. He also recommends not paying the ransom. The information there will help you do what you can do – make sure you're ready for the attack in the first place.

Create and maintain a business continuity and disaster recovery plan. If you don't have one already, ask yourself why. How can compliance be maintained successfully without one? As part of the BC/DR plan, have layered backup storage – from the most expensive storage for the most immediately needed data (e.g. SAN copy), to the least expensive storage for archival records (e.g. tape). Your backup plan should allow you to restore from an incident while meeting your data point and time point objectives.

The real questions that need to be answered are how did this malware get into your organization and can you stop it from happening again? This may mean some remedial security education for people who don't want it. It also means maintaining excellent endpoint security. Locking down endpoint computers is a very good first step. Lock down USB ports and follow security best practices for endpoints as well. Consider scanning and filtering email servers to avoid the primary way by which malware is injected into any organization.

Examine your network perimeter and ensure there are no points of entry or exit that are not monitored – and the logs reviewed daily, including vendor access. If you don't have the resources to read all of the security logs, outsource that activity to a trusted MSSP.

Completely isolate any wireless or guest networks from the business network and healthcare data networks. Review your security policy carefully and look for improvements that can be made – from the top down. Good places to start are personal/non-medical/non-business systems used for browsing, shopping, and other non-work related tasks. Limiting the installation of any software that has not already been pre-approved is another recommended best practice in security. Even end-user access to shared or mapped drives can lead to a disaster. Remove any drive mappings that are not absolutely required to limit what malware can access.

Again many of these are just good security practices in general. A penetration test for a compromised organization is highly recommended to find any other weak points and get them addressed. Engaging Incident Response (IR) services for any suspected issues can prevent an infection from spreading across the organization. Some user re-training may also be needed, and while it may not be the most welcome use of time by employees, the additional training can save an organization from additional headaches in the future. Consider running this training on a yearly basis. Many IR service providers can also provide preventative training and system checkups.

Building a Security Budget and Justifying the Budget

Earlier in this paper we advised on the criticality of knowing your organization's assets to identifying and mitigating threats. Now we want to change your outlook from security being an expense, to an investment. Many organizations in diverse industries have been caught flatfooted due to inadequate funding or management not recognizing the value of

security as an investment. It's absolutely crucial to know how to have the funding conversation with the Security Steering Committees, C-Suite and/or the Board.

Adding to the concern of how to have the funding conversation is the fact that most organizations have not truly thought about aligning the Information Security program with the Information Strategy—at times, because there isn't an Information Strategy. Companies tend to think the data they receive by reviewing common threat data and passing an audit means they have met necessary requirements or have a successful security program – which in most cases is not true. Symantec's MSS Threat team will outline what a strong Information Strategy looks like, and in subsequent whitepapers, how to tie the strategy to a strong Information Security Program that empowers the funding conversation.

Your Program Is Only as Strong as Your Strategy
First and foremost, know your assets, inventory critical people, processes and technologies and be sure to establish metrics to ensure outcomes are met. ISACA (independent security non-profit) promotes the six desired outcomes of IS Governance as critical to your Information Security Strategy. The ISACA desired outcomes are strategic alignment, risk management, value delivery, resource management, performance measurement and integration. Senior management is critical to contributing to and maintaining such a framework to guide the growth and maturity of an enterprise information security program. Only 23 percent of healthcare survey respondents have an ongoing, consistent risk-management program. (Symantec, 2016)

Utilizing frameworks such as COBIT or CMM to help frame your Information Strategy is important to ensure you build and follow best practices. Senior management should have clear strategic goals and objectives so that the Information Security Strategy has defined polices for obtaining said goals and objectives. Clearly stating a company's move to or expansion in cloud services means, customer data, employee processes and security awareness are handled different from traditional non-cloud services. Even as individuals and organizations realize the potential agility and cost savings benefits of cloud computing, concerns about security and availability persist. Whether you want to consume services directly, build your own cloud for internal operations or external reach, or extend into third-party clouds safely and efficiently.

Taking a prioritization approach to your valuable assets is the first step. Then apply cost effective protection to those assets. One must always remember to align the value of the data to the business objective for the business unit goals. Clearly not overlooking business units, inclusive of HR, IT and finance will allow for a comprehensive strategy that addresses potential risks when integrating with business processes. One example would be understanding your risk tolerance. Does your business require as a part of its response and recovery plan to have a hot site (little or no downtime) or warm site (not all data or services available)? Do you know what your response strategy is—threat elimination and reduction, minimizing the impact of the threat or altogether transferring the risk to a third party? When thinking about adding third parties to your operations whether it's an outsource scenario or purchasing cyber insurance, it should always relate back to the Information Security Strategy.

In the case of cyber security, the risk of loss can be defined as the partial or total loss of company or customer data and the premium is the investment required to acquire the necessary software, hardware and cyber security personnel/services to protect the

company from a loss. The investment is the determinable cost up front to provide protection against a future large loss of larger scale with an undetermined major impact and cost to the business. What is known of a loss caused by a cyber-attack is that the impact will be large, expensive and will take time to resolve and put the organization back to its original state. A cyber security strategy and program as an investment provides indemnity against a future large and costly loss caused by a cyber-attack.

Indemnity puts the organization in the same position in which it was immediately prior to the happening of the uncertain event. The only difference is that in the case of cyber security the "event" is not so uncertain — it is usually a matter of when. Therefore, it is recommended that a dedicated portion of any firm's budget is carved out solely for security—an area we will cover in-depth in our next whitepaper in the series.

What's Next?

Symantec Healthcare Whitepapers

Symantec is preparing a series of whitepapers on healthcare information security and assurance topics. These whitepapers are focused on the needs of the healthcare community in applying security to all aspects of healthcare information. Topics planned include:

- Getting That Budget for Security and BYOD in a Medical Setting
- Network Design and Isolation for Security
- Personal Medical Devices
- The Drug Cabinet, X-Ray, EKG, and MRI as an Attack Surface
- Medical Records Online – Compliance vs. Protection

Topics of interest to healthcare providers and users or managers of healthcare information systems are invited to suggest topics of interest for future whitepapers in the series.

Security preparedness is a skill that needs to be learned and practiced. Cultivating a culture of security awareness is key to building a strong defense. Industry roundtables, tabletop exercises, and an on-going dialogue about policy and techniques are all essential components to promote an informed security posture.

Symantec Cyber Security Services

Achieve a Higher Level of Security

Stay ahead of emerging threats and extend your team with our leading cyber threat experts for global threat and adversary intelligence, advanced threat monitoring, cyber readiness, and incident response. Bolster your security posture with the capabilities of our experts around the world.

Shorten the time between detection and response, reduce operational costs, and proactively counter emerging threats.

SOC Consulting Services – Symantec Consulting Services works with organizations to build and extend their SOCs – at whatever point they are on the maturity curve. Symantec consultants draw upon best practices acquired through their global cyber operations engagements with business and governments globally, as well as their SOC operations experience worldwide. Leveraging their deep expertise, Symantec consultants assess customers' cyber operations functions against Symantec's SOC maturity model and provide recommendations to accelerate improvement and change.

Global Threat Intelligence -- Symantec DeepSight™ Intelligence provides a deeper understanding of the threat landscape so organizations can make more informed decisions to proactively mitigate cybersecurity risk. Technical and strategic intelligence keeps security and intelligence teams informed of industry-specific vulnerabilities, providing advanced analysis of attacks and sharing the motivations and techniques of threat actors. You can access DeepSight through the Portal, API, Datafeeds, and customized Directed Threat Research.

Continuous Threat Monitoring and Analytics -- Symantec Managed Security Services (MSS) enables organizations to reduce false positives and focus on critical alerts by using advanced analytics, actionable threat intelligence, and a seasoned team of global security experts who provide 24x7 threat monitoring and proactive threat hunting. Symantec assigns to each customer a designated Service Manager and analyst team who are experts in the customer's industry, providing continual collaboration and partnership.

Fast and Precise Incident Response -- Symantec Incident Response Services work with organizations around the globe to validate and respond to incidents with speed and precision. Drawing from years of experience and leveraging powerful threat intelligence and industry-accepted forensics tools and procedures, Symantec helps organizations return to business as quickly as possible and strengthens an organization's overall ability to detect and eradicate future threats.

Organization-wide Cyber Skills Development -- Symantec Cyber Skills Development Services increase organizational resiliency to cyberattacks by training and assessing both technical and non-technical employees. This portfolio trains and assesses end-user susceptibility to attacks including those that leverage social engineering tactics such as spear phishing. Additionally, scenario based, live-fire training environment provides a safe environment for technical users to understand the current threat landscape, motives and methodologies of the adversary.

References

Healthcare IT Security and Risk Management Study, Symantec and HIMSS (2015). Retrieved from https://resource.elq.symantec.com/LP=2713?cid=70138000000jLvUAAU&mc=197213&ot=wp&wpn=177&tt=ws on May 3, 2016.

The Diamond Model of Intrusion Analysis, Betz, C., Caltagirone, S., and Pendergast, A. Hutchins, E., Cloppert, M. and Amin, R., "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Proc. 6th Int'l Conf. Information Warfare and Security (ICIW 11), Academic Conferences Ltd., pp. 113–125; retrieved from http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LMWhite-Paper-Intel-Driven-Defense.pdf on Aug. 12, 2015, 2010.

Information Systems Audit and Control Association (ISACA). https://www.isaca.org

Johnson, Emily "5 Reasons Cybercriminals Target Healthcare," (2016, April). *Dark Reading.* Retrieved from http://www.darkreading.com/endpoint/5-reasons-cybercriminals-target-healthcare/d/d-id/1325210 on July 9, 2016.

Leventhal, Rajiv. "Data Security in 2015: A Need to Be Proactive." Healthcare Informatics. Vendome Healthcare Media, n.d. Web. 12 Sept. 2016.

"Microsoft technology solutions for cybersecurity," Microsoft Corporation, retrieved from http://download.microsoft.com/download/D/3/0/D30E9D65-7330-4DD3-B6A7-28BAE8381AE4/CybersecurityTechnology.pdf on Sep 14, 2015, 2010.

Mohammed, D., Mariani, E., Shereeza, M., "Cybersecurity Challenges and Compliance Issues within the U.S. Healthcare Sector," International Journal of Business and Social Research, Vol 5, Issue2, 2015.

Moore, J. "Health care providers look to improve security incident response," iHealthBeat, 2013.
O'Gorman, G., & McDonald, G. (2012, November). *Symantec Security Response.* Retrieved March 28, 2016, from Ransomware: A Growing Menace: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

Savage, K., Coogan, P., & Lau, H. (2015, August). *Symantec Security Response.* Retrieved March 28, 2016, from The Evolution of Ransomware: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

Symantec. Retrieved April 8, 2016, from Cybersecurity in Healthcare: Why It's Not Enough, Why it Can't Wait: https://www.symantec.com/content/dam/symantec/docs/infographics/symantec-healthcare-it-security-risk-management-study-en.pdf

Symantec. The Sign of a Safe Cloud. http://www.symantec.com/cloud-computing-software/

Vogel, DJ. (2012, September). “A Hackers Bucket List”. Retrieved May 2, 2016 from 403 Blogs: http://blog.403labs.com/post/32348548783/a-hackers-bucket-list