Trend Micro Healthcare Compliance Solutions

How Trend Micro's innovative security solutions help healthcare organizations address risk and compliance challenges.

Introduction

The foundation of any good information security program is risk management. Organizations need to understand the following:

- What information is being stored, processed or transmitted
- What are the confidentiality, availability and integrity requirements of the information
- What are the compliance requirements of the information and penalties for failure
- How to implement people, process and technology controls to address the requirements

In a healthcare setting the protected health information (PHI) is the primary focus of information technology (IT) risk management practices. Traditionally, sensitive health information has flowed through the organization via paper records. Maintaining and protecting these records relied heavily on people and processes. Risks to the unauthorized access, modification or destruction of information existed but the impact was typically only one or a handful of individuals on average. With the increased adoption of technology in healthcare such as electronic medical records, health information exchanges, and networked medical devices, the risk to PHI increases in both likelihood of unauthorized disclosure and impact to the organization given the greater amount of data accessible. Further, legislation introduced in September 2009 increased the scope and penalties of compliance regulations.

The Importance of Privacy in Healthcare

Security and privacy provide the basis for enabling trust in the healthcare industry. Security enables privacy which in turn allows patients to trust providers of care with their sensitive information. In fact, the Institute of Medicine (IOM), a respected nonprofit which conducts research in the healthcare space stresses the importance of privacy and its link with patient care:

> *"breaches of an individual's privacy and confidentiality may affect a person's dignity and cause irreparable harm…and [unauthorized disclosures] can result in stigma, embarrassment, and discrimination."* [1]

In this statement, the IOM directly links patient harm to privacy. If privacy cannot be reasonably maintained and assured there is an increase in the potential for harm. And unlike breaches of personally

[1] IOM: Beyond the HIPAA Privacy Rule—Enhancing Privacy, Improving Health Through Research, January 2009, http://www.iom.edu/Reports/2009/Beyond-the-HIPAA-Privacy-Rule-Enhancing-Privacy-Improving-Health-Through-Research.aspx

identifiable or financial information, individuals cannot easily be made whole or protected when patient information is disclosed to an unauthorized individual. There is no health record monitoring; what a neighbor of colleague discovers about another's health cannot be undone; restoring a health record after it has been used for fraudulent activities can be painstaking and may result in denial of care or medication.

In another report by the IOM, Crossing the Quality Chasm[2], six aims for improvement are defined as a means of reducing the burden of illness, injury, and disability, improving the health of individuals in the U.S. These aims are focused on healthcare being:

Integrity
- **Safe**: avoiding injuries to patients from the care that is intended to help them.
- **Effective**: providing services based on scientific knowledge to all who could benefit, and refraining from providing services to those not likely to benefit.

Confidentiality
- **Patient-centered**: providing care that is respectful of and responsive to individual patient preferences, needs, and values, and ensuring that patient values guide all clinical decisions.
- **Equitable**: providing care that does not vary in quality because of personal characteristics such as gender, ethnicity, geographic location, and socioeconomic status.

Availability
- **Timely**: reducing waits and sometimes harmful delays for both those who receive and those who give care.
- **Efficient**: avoiding waste, including waste of equipment, supplies, ideas, and energy.

As noted above, there is a close link with many of these aims to the core pillars of security: confidentiality, integrity, and availability (CIA). Confidentiality of information enables equitable care by reducing or removing individuals' biases. Integrity of information enables effective care by keeping information in its intended state, not being altered without knowledge or authorized intent by a care provider. Availability of information enables clinicians to access information when and where he or she needs it to make decisions about appropriate care needed by a patient.

While the regulations are not as explicit in the linkage between safety and care with privacy and security, the intent is the same.

Regulations and Compliance in Healthcare

State of Security in Healthcare

With the volume of security compliance requirements and the costs associated with disclosure after a breach, one might expect the industry to be fairly mature with respect to protecting PHI. Unfortunately, breach and benchmark data indicates otherwise.

[2] Crossing the Quality Chasm: A New Health System for the 21st Century, March 2001, http://www.iom.edu/Reports/2001/Crossing-the-Quality-Chasm-A-New-Health-System-for-the-21st-Century.aspx

Breaches on the Rise

Since the Breach Notification rule went into effect in September 2009, over 233 breaches are recorded. In 2010, the average number of breaches per month was almost 20. And the total number of records and individuals affected is 6.74 million[3]. Of the types of organizations experiencing breaches, physicians practices and hospitals are the biggest targets accounting for 25% and 37% respectively. Health insurance plans however account for the greatest loss of PHI with over 50% of breached records originating from these organizations. Over 50% of the breaches stem from the theft of laptops, removable media and desktops.

Looking at Verizon Business' annual data breach investigation report, some 38% of breaches and 94% of records breached involved the use of malicious software, with about half of the breaches involving viruses with no customization. The use of social techniques such as email phishing, where a malicious link is sent in an attempt to gather sensitive information like passwords from unsuspecting users, occurred in almost 30% of breaches. Hacking is also a significant issue that is steadily increasing since 2005 when Verizon began capturing this data point, and now accounts for 40% of breaches.

Cost of a Breach

What is the effect on organizations that experience a breach? According to a study conducted by the Ponemon institute[4], the cost per record of a breach in healthcare is $204—this is comprised of a direct element ($60) and an indirect element ($144). This includes both the cost of the actual notification, sending out letters, and associated costs like credit monitoring, forensic analysis, remediation and reputational damage. The Office of Civil Rights (OCR), which is responsible for enforcing the HIPAA rules, may also fine organizations for HIPAA violations up to $50,000 per violation and up to $1.5 million per year. In addition, state attorneys general are now also able to enforce the HIPAA rules and can enforce additional penalties on organization for violating the rules. In July 2010, the Connecticut Attorney General's office assessed a fine of $250,000 against Health Net. More recently, Massachusetts General Hospital reached a settlement with OCR for $1,000,000 for a breach in 2009 involving 192 patient records. Real consequences for real organizations that could, in many cases, be mitigated with fundamental security controls and technologies.

Managing Risk

A tenet of the HIPAA Security rule—discussed in greater detail later in this paper—is managing risk through reasonable and appropriate controls. This too is fundamental to IT risk management, which dictates that organizations assess the vulnerabilities present and the threats to those vulnerabilities and identify the appropriate techniques to manage those risks (e.g., controls, insurance, acceptance). By simply looking at the breach data listed above, however, it is fairly clear what some of the high risks are to organizations in healthcare: malware, unencrypted transmissions, unencrypted storage on mobile devices, social engineering, data loss, and hacking. Given this, what is reasonable and appropriate for organizations is to implement controls to address these risks. Considering the cost of breach notification

[3] As of February 2011

[4] http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/US_Ponemon_CODB_09_012209_sec.pdf

and the increasing penalties, it is not only sound security and risk management practice but sound business practice.

Addressing Compliance

From a compliance perspective, healthcare organizations of all sizes and segments must address certain federal requirements, many of which were just recently introduced or have just recently changed. Specifically this paper looks at the following with supporting rationale:

- HIPAA Rules—The HIPAA Security, Privacy, Penalties and Enforcement rules are all being updated as part of the HITECH Act released in 2009. These changes impact all covered entities and more significantly all business associates and subcontractors working with covered entities, as they will now be directly subject to HIPAA. All healthcare organizations, large or small, are required to be in compliance with the current rules and with the new rules.
- HITECH Act—As mentioned above, the HITECH Act impacted the HIPAA rules but also had more widespread objectives and impacts on healthcare as an industry, intent on increasing the adoption of health information technologies. This includes establishing health information exchanges at state and national levels, increasing the use of electronic health records systems within hospitals and physician practices, and providing patients with more control over how their information is used, among many other changes.
- Breach Notification—The Breach Notification requirements are yet another result of the HITECH Act. Breach Notification imposes new requirements on healthcare organizations and business associates to notify affected patients, media outlets, and the DHHS when they experience a breach involving PHI. Notification must be provided within 60 days but without unreasonable delay. Since Breach Notification went into effect in September 2009, well over 200 instances of breaches have been logged, with each breach affecting 500 individuals or more.
- Meaningful Use—Under HITECH, CMS was charged with establishing an incentive program around the meaningful use of electronic health records (EHR) systems. This incentive program outlines requirements and thresholds for both the technology itself and the organizations adopting the technology to ensure the systems are being used in meaningful ways. While there are direct incentives available up through both Medicare and Medicaid, there are also penalties beginning in 2015 for those organizations that have not successfully adopted EHR technology.
- HITRUST—HITRUST, the Health Information Trust Alliance, and the HITRUST Common Security Framework (CSF) are recent additions to the healthcare information security and compliance landscape. HITRUST was established in 2008 with the objective of enabling trust in the healthcare industry. The CSF is a framework designed to provide prescriptive, comprehensive guidance on implementing reasonable and appropriate security controls based on risk and agreed to by the broader industry. Since its inception, HITRUST has released a CSF Assurance Program, which is a means of assessing high risk areas of organizations as a means of satisfying risk management requirements such as those in HIPAA and Meaningful Use.
- PCI—PCI, the Payment Card Industry, and the PCI Data Security Standard (DSS) are a more broadly focused, international industry group and set of requirements for payment card (e.g., credit card) processors and merchants accepting those cards. Many healthcare organizations,

such as hospitals and physician practices, accept credit cards as a form of payment for healthcare services. Considering this, many healthcare organizations are subject to this rigid and strict set of requirements which recently went through an update in late 2010 to version 2 of the standard.

A more detailed explanation of each of the standards and regulations is provided in the following sections.

HIPAA

Health Insurance Portability and Accountability Act of 1996

HIPAA, enacted on August 21, 1996, was designed to improve the continuity of coverage and care services while simplifying the administration of healthcare. HIPAA established a set of national privacy and security standards for the protection of certain health information.

The HIPAA Privacy rule, which went into effect in 2003, requires that personal health information be protected and kept confidential. Access to patient information must also be limited to only those who are authorized and only on a need-to-know basis. HIPAA also required the development and adoption of standards to secure protected health information (PHI) while in the custody of 'covered entities', as well as in transit between covered entities and from covered entities to others. These requirements that became the HIPAA Security rule went into effect in 2005.

The HIPAA Privacy rule (§164.530(c)(1) Standard: Safeguards) informs the Security rule requiring "a covered entity must have in place appropriate administrative, technical and physical safeguards to protect the privacy of protected health information." The Privacy rule sets the requirement; the Security rule provides requirement for these three safeguards.

Generally, the Security Rule requires a covered entity to:

- Ensure the confidentiality, integrity, and availability of all ePHI the covered entity creates, receives, maintains, or transmits
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule
- Ensure compliance by its workforce

These protections are set forth as administrative, physical and technical safeguards as mentioned in the privacy rule and described as follows:

- "Administrative safeguards are administrative actions and policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."

- "Physical safeguards are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."
- "Technical safeguards mean the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."

To achieve the abovementioned safeguards, organizations must start with a risk analysis to identify threats to the confidentiality, integrity or availability of ePHI and implement security measures to protect against these threats. The subsequent administrative, physical and technical safeguards listed within the rule provide the basis for the security measures to implement. Many of these safeguards, however, are addressable meaning the organization and the assessment must inform whether the safeguard is reasonable and appropriate to implement. The assessment, decision and rationale must be documented. This documentation along with all other documentation required by the standard (hardcopy or electronic) must be retained for a minimum of six years from the date it was created or the date it was last in effect, whichever is later.

HITECH Act

Health Information Technology for Economic and Clinical Health Act of 2009

HITECH, enacted in 2009 as part of the American Recovery and Reinvestment Act (ARRA), includes coverage (COBRA and Medicaid), health IT and privacy provisions designed to improve the quality of the US health care system while lowering its costs. With respect to the health IT provisions, the federal and state governments are investing in both a nationwide and state electronic health information exchanges and encouraging hospitals and physicians to adopt electronic medical records systems to improve care and better facilitate information exchange. The Act also strengthened federal privacy and security law to protect health information from misuse as the health care sector increases use of health IT. It also resulted in the modification of the HIPAA Privacy, Security and Enforcement rules and created the Breach Notification rule. Generally these changes include:

- Requiring that an individual be notified if there is an unauthorized disclosure or use of their health information
- Expanding the scope of the HIPAA rules to directly apply to entities that store, process or transmit PHI on behalf of providers and insurers
- Providing transparency to patients by allowing them to request an audit trail showing all disclosures of their health information made through an electronic record
- Requiring that providers obtain authorization from a patient to use their health information for marketing and fundraising activities
- Strengthening the enforcement of HIPAA by increasing penalties for violations and providing greater resources for enforcement and oversight activities

Breach Notification

Requiring HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

Subtitle D of Division A (entitled 'Privacy') of the HITECH Act required HHS to create new regulations for breach notification by covered entities and their business associates in the event there is an unauthorized disclosure of unprotected PHI. The Breach Notification Interim Final Rule became effective on September 23, 2009, and remains in effect until a final rule is issued by HHS.

A breach is defined by the rule as "an impermissible use or disclosure under the Privacy rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual." Covered entities and business associates need only to provide notification if the breach involved unsecured PHI. Unsecured PHI is defined as PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of an approved technology or methodology. Currently the only approved means of securing PHI is encryption or destruction. Thus adequately encrypting or destroying PHI may grant organizations safe harbor from notification in the event of a breach.

When a breach occurs and on the first day the organization discovers the breach—or should have discovered a breach exercising reasonable due diligence—the organization has 60 days to notify the individuals whose information was involved in the breach, however notification must be provided without unreasonable delay. When 500 or more individuals are involved by state, the organization is required to notify major media outlets, in other words provide public notification. When 500 or more individuals, irrespective of state or jurisdiction, are involved, notice to the Secretary of HHS must be provided immediately. If fewer than 500 individuals total have been affected by a breach, then the organization must still report to the Secretary, but it may be in the form of a log on an annual basis.

There are certain exceptions to the current rule whereby an organization does not need to provide notification for a breach of unsecured PHI, commonly referred to as "safe harbor." Safe harbor is granted when either of the following is true:

- The patient information is encrypted and subsequently inaccessible by an unauthorized individual
    - Encryption systems must meet the NIST SP 800-111 standard for stored data to be deemed secure[5]
- The patient information has been disposed of in a secure manner, such as degaussing hard drives or shredding paper records
    - Electronic media have been cleared, purged, or destroyed consistent with NIST SP 800-88[6]

It is important to note that notification is always provided by the covered entity, even if a business associate was involved and experienced the breach. While the rule requires business associates to notify the covered entity of the breach, it is the covered entity's responsibility to notify the individuals, media and HHS in accordance with the requirements mentioned above.

[5] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html
[6] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html

Meaningful Use

Demonstrating the use of certified EHR technology in meaningful ways that facilitate the exchange of health information and improve the quality of patient care.

In addition to the HIPAA rule changes, HITECH introduced programs and funds for the enhanced privacy and security protections, standards development and certification infrastructure for EHRs. The Centers for Medicare and Medicaid Services (CMS) charged with providing guidance and defining requirements for professionals and hospitals that would adopt this EHR technology, has established an incentive program along with a number of categories, objectives, and measures for what it means to be a meaningful user of EHR technology and receive incentive payments. The requirements to receive funds are defined in three stages, with the first stage already defined and the other two to be defined at a future date during the program—stage 2 to be issued in 2011 and stage 3 in 2013.

Eligible professionals (EPs) may seek incentive under Medicare or Medicaid (not both):

- Medicare: Up to $18,000 in calendar year 2011 or 2012, to five year cap of $44,000
- Medicaid: Maximum of $63,750 over six years, $21,250 maximum in first year

Eligible Hospitals may receive both Medicare and Medicaid payments based on the following formula:

- base of $2 million for up to 1,149 acute care inpatient discharges for prior 12 months
- plus $200 for each additional discharge up to 23,000
- maximum of $6,370,200, plus transition factors

Of the stage 1 criteria for EPs and eligible hospitals, a core set and a menu set are defined. The core set includes 15 objectives for providers and 14 objectives for hospitals, all of which must be met. The menu set includes 10 objectives for both EPs and hospitals, five of which must be chosen and met.

Privacy and security is a core set for stage 1:

Category "[To] ensure adequate privacy and security protections for personal health information."

Objective "Protect electronic health information created or maintained by certified EHR technology through the implementation of appropriate technical capabilities."

Measure "Conduct or review a security risk analysis per 45 CFR 164.308(a)(1) and implement updates as necessary and correct identified security deficiencies as part of the EP's, eligible hospital's or CAH's risk management process."

The measure listed above relates to the HIPAA Security rules requirements for risk analysis and risk management, essentially requiring EPs and hospitals to conduct a risk analysis and implement updates to ensure the confidentiality, integrity, and availability of ePHI, protecting against threats and unauthorized disclosures.

HITRUST Common Security Framework (CSF)

Developed in collaboration with healthcare and information security professionals, the Common Security Framework (CSF) is the first IT security framework developed specifically for healthcare information.

The Health Information Trust Alliance (HITRUST) arose from the belief that information security is critical to the broad adoption, utilization and confidence in health information systems, medical technologies and electronic exchanges of health information.

HITRUST is collaborating with healthcare, business, technology and information security leaders, to build this greater level of trust between organizations through a common security framework and program for assessing and reporting information security controls. In 2009, HITRUST delivered the first Common Security Framework (CSF) to the industry. The CSF is not a new standard, this is a common misconception. The CSF is a framework which normalizes and cross-references the requirements of existing standards and regulations including federal (e.g., HIPAA, HITECH, Meaningful Use), state (e.g., Massachusetts, Nevada), third party and business (e.g., PCI, ISO, JCAHO) requirements. Additionally, HITRUST has been able to add a degree of prescriptiveness in security requirements that have been traditionally lacking, which makes adoption and compliance more consistent and simpler. The CSF is also scalable based on risk and complexity, accounting for different sizes of organizations and the types of systems used, providing the right level of control based on these factors.

In conjunction with the CSF, HITRUST established the CSF Assurance Program whereby organizations can assess and report their risk exposure against a subset of required controls of the CSF. The CSF Assurance Program provides consistency in the currently disparate assessment and reporting processes utilized by healthcare organizations. Through one program and against once set of requirements, organizations can streamline the number of assessments they conduct each year and how they report the results to third parties, while also managing risk. Since the Assurance Program based on the CSF which itself is based on existing standards and regulations, HITRUST provides organizations with an excellent solution for conducting risk assessments and managing risk as required by the HIPAA Security rule and Meaningful Use. The Office of Civil Rights (OCR) has in fact issued guidance[7] recognizing HITRUST and the CSF as a viable option for conducting a risk analysis under the HIPAA Security rule.

While the CSF and CSF Assurance Program are merely de facto requirements now, both have seen continued growth in support and adoption since HITRUST initially launched each respectively. HITRUST itself is supported by executive, industry leadership from organizations like UnitedHealth Group, WellPoint, Humana and Express Scripts among others and has a growing number of members in its online community.

PCI DSS

An actionable framework for developing a robust payment card data security process to help organizations ensure the safe handling of cardholder information at every step.

[7] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

The Payment Card Industry (PCI) Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards including the Data Security Standard (DSS). The Council's five founding global payment brands are American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. Each of these companies have agreed to incorporate the PCI DSS as the technical requirements of each of their data security compliance programs, meaning any organization of any size that wishes to do business with these organizations (i.e., accept payment cards) must comply with the DSS.

The PCI DSS provides an actionable framework for developing a robust payment card data security process, including prevention, detection and appropriate reaction to security incidents. The DSS includes twelve requirements for any organization that stores, processes or transmits payment cardholder data. These requirements specify the framework for a secure payments environment. For purposes of PCI compliance, their essence is three steps: assess, remediate and report.

To *assess* is to take an inventory of your IT assets and processes for payment card processing and analyze them for vulnerabilities that could expose cardholder data. To *remediate* is the process of fixing those vulnerabilities. To *report* entails compiling records required by PCI DSS to validate remediation and submitting compliance reports to the acquiring bank and global payment brands you do business with. Carrying out these three steps is an ongoing process for continuous compliance with the PCI DSS requirements. These steps also enable vigilant assurance of payment card data safety.

PCI provides and maintains a Self-Assessment Questionnaire (SAQ) which is a validation tool for merchants and service providers who are not required to do on-site assessments for PCI DSS compliance. There are four SAQs specified for various situations depending on how the merchant interacts with the payment card and its information.

For those organizations required to conduct on-site assessment, the Council provides programs for two kinds of independent experts: Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV). QSAs have trained personnel and processes to assess and prove compliance with the PCI DSS. ASVs provide commercial software tools to perform vulnerability scans for payment card systems.

Each member organization of PCI defines different classifications of merchants requiring a different level of assessment and reporting based on the classification. Generally speaking, large merchants processing multiple millions of transactions for a particular merchant annually will be classified as level 1, meaning the organization must conduct a third party assessment and report annually. Merchants which fall in levels 2 through 4 generally process low millions to thousands of records annually and typically are only required to conduct a self-assessment. A quarterly network scan is required in almost all instances.

Trend Micro's Security Solutions

Trend Micro is a leading provider of information security technologies designed to protect organizations from the increasing threats to sensitive information like PHI. Trend Micro's overarching set of solutions scale to small, medium and large organizations, tailoring their products to the needs of each kind of organization.

Trend Micro is also more than just a vendor; they have truly positioned themselves as a trusted advisor when it comes to managing security and compliance in healthcare. With all of Trend Micro's products, a full support team is available to facilitate the successful implementation and deployment of the security solution. In certain circumstances, as is discussed in this paper, Trend Micro even provides a team during the lifecycle of the product, augmenting an organization's security team and assisting in the monitoring and management of security within the organization. Trend Micro also exhibits a strong focus on addressing emerging technologies and the associated risks. Virtualization of organization's server industry is an attractive means of providing IT resources without the high cost of physical devices. Trend Micro embraces this across a majority of their solutions, providing the solution as either a traditional hardware or software device or as a virtual appliance on VMware. In this area, virtualization also introduces new risks that organizations are still struggling to address. Trend Micro's solutions provide protection of both virtual, physical, and hybrid environment seamlessly. Virtualization is not just a technology for the data center either; virtual desktop infrastructure (VDI) is the practice of hosting a desktop operating system within a virtual machine. VDI is having a major impact in healthcare as a means of providing shared workstations within a clinical setting, allowing physicians and nurses to move from one terminal to the next accessing the same desktop and applications across the facility. While the desktops are virtual the threats are real, requiring protection from malicious software for example.

The cloud is another growing area, often used for lowering the operating costs to organizations. Trend Micro leverages the cloud in a unique way with their Smart Protection Network ™. The Smart Protection Network is a cloud-based infrastructure enabling better protection of organizations while reducing the resource impact. This unique technology is a global network of devices, sensors and intelligence leveraged across Trend Micro's security solutions and services to enable protection before the threat even reaches the organization's front door. Organizations using Smart Protection Network-aware solutions can also opt-in to providing smart feedback to the network, acting as yet another data source of good and bad content. This multi-layered solution uses sophisticated algorithms and technologies to identify a file's, website's or sender's reputation and block malicious content. Because it is all done in the cloud powered by Trend Micro, organizations get immediate protection that is always up-to-date, without the demand on system resources of traditional products.

Because the Smart Protection Network aggregates data on emails, files, and websites, it is able to correlate these threat vectors to enhance protection across all mediums versus working in silos like most security solutions. For example, spam is often a source of malicious URLs whereby a spammer sends a link masked as a known, good website but is truly a malicious website. With email reputation, the Smart Protection Network would flag the email as malicious spam and block all future instances from the sender. The web filter, however, would also pick up the URL within the email and analyze the website's reputation, visiting the page and downloading any content. If malicious content is discovered, the URL will too be flagged and blocked in all future instances. Finally, if on the website a malicious file is downloaded and discovered, the file reputation would also be updated, again blocking all future instances of the malicious file via email, web, or other. Many of the solutions below leverage Trend Micro's Smart Protection Network to keep organizations secure.

With the emergence of new encryption requirements it is crucial that any security solution meets the standards that have been adopted. Since these are based on federal guidance, Trend Micro's acquisition of Mobile Armor provides a robust and superior data encryption solution. The solution will exceed the NIST specifications that have been referenced in healthcare regulations and generally enable proper risk management in accordance with HIPAA.

Although, not covered in this review, Trend Micro's new product SecureCloud offers a data encryption and key management solution for organizations currently using or evaluating the use of the cloud. While there are a number of benefits to using a cloud in lowering operating costs, a barrier to entry for many organizations particularly in healthcare is the security of data stored in the cloud. In many instances a cloud provider will offer to encrypt data, as an additional service, but there is still risk because they also manage the keys. SecureCloud leverages the integrity of Trend Micro as a provider of security and data protection solutions and also separates each organization's duties to better manage risk. The cloud provider hosts the encrypted data and Trend Micro manages the encryption and key management on behalf of the healthcare organization.

Solutions Enabling Compliance

The solutions listed below are designed for a specific type of organization: small, medium, or large / enterprise. The features and functions of each solution are tailored with the organization needs in mind, where small organizational solutions are designed for simplicity, ease of use and limited resources and enterprise grade solutions are designed for centralized, robust management and best-in-class security. It is critical to understand this distinction both from a usability perspective and from a risk perspective. Each solution enables organization to address compliance and their overall risks based on their environment—the threats and impacts for a large organization are not equitable to those of a small organization and so the technologies and controls implemented should be adjusted accordingly.

What follows is an introduction and overview of five of Trend Micro's security solutions:

1. InterScan Messaging Security Virtual Appliance (ISMVA)
2. WorryFree
3. OfficeScan
4. Mobile Armor (Trend Micro Endpoint Encryption [TMEE])
5. Deep Security
6. Threat Management Services

For each solution, an overview of the security features is discussed, a description and diagram of how the solution integrates into healthcare is detailed and a compliance scorecard is provided. This enables organizations to understand what each product does, how it fits into the environment and how it aligns organizations with regulatory compliance requirements in healthcare.

Authors

Cliff Baker
Managing Partner
Meditology Services

For the past 16 years, Cliff has worked with leading healthcare companies across all sectors of the industry and served as an executive advisor for key industry affiliations and companies. He is a sought after contributor to various health IT and information security forums including the sixteenth national HIPAA Summit among others. For the past two years, Cliff has served as the Chief Strategy Officer at the HITRUST Alliance, an industry consortium which established the most widely adopted information security and compliance framework for the healthcare industry. Prior to joining HITRUST, Cliff led the southeastern healthcare advisory practice for PricewaterhouseCoopers.

Chris Hourihan
Director
Meditology Services

Chris is seasoned professional in the healthcare industry who is consistently delivered quality results on time in the projects he leads. These include information security and compliance risk assessments, security and privacy training, and third party security management program development. His experience has focused almost exclusively in the healthcare industry and he has collaborated with a wide variety of organizations from the provider, payer, vendor, exchange, and clearinghouse sectors. His focus has traditionally been on simplifying compliance and evaluating security risks, addressing standards and regulations including ISO 27001/2, HIPAA, HITECH, CMS, PCI, FTC, State requirements, and Meaningful Use. In addition to tactical deployment and project management, Chris has held strategic roles in defining services and solutions to drive long range business success. His commitment to this industry and his own growth in knowledge and experience is demonstrated through his presentations and whitepapers on issues around information security breaches, medical device security, and streamlined risk assessments for meaningful use.