Symantec and Intel


Who should read this paper
Information Technology Management and Staff in the Healthcare Industry
Symantec and Intel

Content
Risk Management .......................................................... 1
Risk Assessment .......................................................... 3
Security ................................................................. 6
Symantec and Intel Solutions Mapping .................................. 7
References and Further Education ...................................... 8
**Risk Management**

This document will review the existing compliance challenges and IT risks faced by today’s healthcare organizations by reviewing both, the current regulatory environment as well as the evolving threat landscape.

Managing these risks is an essential step in operating any business. However, many healthcare organizations have limited budgets available to achieve their compliance, privacy and security goals. The challenge is how best to allocate this budget and most effectively use the available resources. A formal and comprehensive risks assessment enables organizations to model and prioritize risks objectively and to determine where best to allocate limited resources. Without such an approach, organizations risk over-spending in some areas and neglecting others, leaving weakest links that can lead to security incidents such as breaches. In general, no security safeguard can be bulletproof. For example, if poorly implemented, encryption can be vulnerable to weak, reused, shared, or written down passwords, resulting in residual risk that may need to be further mitigated through the application of supplemental security controls in a multi-layered, defense-in-depth approach. With this approach the question becomes how much residual risk is acceptable to the healthcare organization?

Risk assessments enable a measured approach based on baselines of acceptable risk, typically defined by the senior management of the healthcare organization in the privacy and security policy of the organization. In the absence of such a measured approach, privacy and security risks becoming a budgetary black hole for the organization.

Eliminating all threats is impossible and because of continual change in an organization, its IT infrastructure, and compliance requirements, businesses will periodically need to conduct a risk analysis to determine their possible exposure and how best to manage risks appropriately to an acceptable level.

Looking at the risks faced by today’s healthcare providers, a number of considerations come into play. On the highest level there is risk to the patient and risk to the business but there are also specific risks factors affecting infrastructure and IT systems. Correspondingly, the threat vectors can range from natural disaster to malware outbreaks or data breaches, and even the risk of non-compliance and its legal, financial, and reputational consequences.

IT infrastructure is growing more complex, information needs to be exchanged across care providers, and clinical end users require secure and reliable access anytime and anywhere and on a variety of corporate-issue and personal devices.

At the same time, external threats are increasing at a rapid pace. As cyber crime is being taken over by international criminal organizations and governments, we see hackers are becoming more sophisticated and malware is not only growing exponentially, but also becoming targeted and stealthy.
Healthcare providers need to address all aspects of potential risks to assure high availability, security and privacy, business continuity and disaster recovery as well as minimize the risk to their business, reputation, and patient population. According to the Georgia Tech Information Security Center (GTISC) mobile devices and social networking, botnets, and cyber threats targeting physical systems are three of the main cyber security target areas for 2011:

- **Cyber Threats Targeting Physical Systems:** As infrastructure services such as electric grid and utilities become increasingly interconnected, they will face greater risk of disruption and misuse. In addition, cyber attacks are also a growing risk for healthcare systems as integration and connectivity becomes increasingly complex. What’s more, the ability of updating the security protection of systems and devices in these environments may be limited and they may be subject to regulatory constraints.
- **Botnets:** Specifically large-scale attacks that utilize more targeted malware to evade detection; in addition, cyber criminals are now making more efficient use of malicious software and have been re-launching previously thwarted attacks.
- **Mobile Devices and Social Networking:** As more open mobile device platforms grow in popularity and more applications become available, these devices will become more attractive targets of attacks. In addition, cyber criminals are using publicly available information gleaned from social networking accounts to lure users into handing over personal and sensitive information in spear phishing attacks.

To compete effectively in business it is necessary to understand the competition. Similarly, to adequately secure healthcare organizations it is necessary to understand the threat agents, and the value of the healthcare data they seek to acquire. Better understanding of threat agents enables more consistent prioritization of risks, and improved ability to triage the most likely risks from the hypothetical distractions.

Electronic Protected Health Information (ePHI) has become a lucrative target for malicious attack and insider theft. The motivation ranges from prescription fraud, financial fraud, blackmail and extortion, celebrity snooping to health insurance fraud to identity theft. The street cost for a stolen medical record is valued much higher than other forms of sensitive data at approximately $50, while the cost of a Social Security Number is only approximately $1. Similarly, the payout for medical identity theft is also much higher at $20,000 vs $2,000 for non-medical identity theft. An analysis of all PHI breaches over 500 records and publicly recorded between September 2009 and the end of 2010, found 225 security breaches affecting 6,067,751 individuals, an average of ~27,000 individuals per breach. Two-thirds of all records breached resulted from laptops or other portable media devices and 40% involved business associates; 61% of breaches were a result of malicious intent. Unique to healthcare is the mix of traditional IT endpoints (servers, PC’s, and laptops) with dedicated purpose systems, i.e. medical devices used for diagnosis and treatment. Increasingly building on standard computing platforms, these devices are as vulnerable to attacks as traditional IT systems. However, they are much more prevalent, more difficult to protect, and once infected their malfunction can have significant impact on patient care or even lives. In recognition of these special circumstances, Symantec and Intel are working with healthcare providers, manufacturers, industry organizations, and regulatory bodies to provide security and management solutions for medical devices.

3- Ponemon Institutes 2010 Annual Study: US Cost of a Data Breach
Mobile and Cloud

Mobile and cloud computing are rapidly growing trends, driven by improved clinician mobility, improved patient care, lower cost, and improved healthcare organization IT agility. Mobile devices include smart phones, tablets, and laptops. Most healthcare organizations view these devices as being either "critical" or "important" for the delivery of patient care. In healthcare the cloud data center is often managed by the EHR software vendor.

The traditional perimeter approach to security where buildings and firewalls mark the physical and logical security perimeters around healthcare organization and its PHI is being challenged by mobile and cloud computing. Mobile computing enables anywhere, anytime access to PHI inside and outside of the secure perimeter, while cloud computing stores the PHI outside of the traditional perimeter in the cloud provider’s data center.

With the many benefits mobile and cloud computing offer, they can also put an organization at an increased risk of data breach. Mobile devices are often at increased risk of loss, theft, unauthorized use or use of unsecured wireless. According to Juniper’s Networks Malicious Mobile Threats 2010/2011 Report, mobile devices are also at increasing risk of malware infection. Cloud computing can introduce risks to the confidentiality, integrity or availability of sensitive healthcare information. The challenge to healthcare organizations is how to safely embrace mobile and cloud computing, enabling them to realize the benefits while avoiding security incidents such as breaches.

Keeping data secure in mobile and cloud environments is not only a challenge, but a critical requirement under Federal and State law. Organizations using mobile and cloud computing must ensure compliance, data security, and monitoring and audit ability across all applications and purposes. They must adopt a more formal, process oriented approach towards traditional, mobile, and cloud management and security to include:

- Conducting a thorough inventory of sensitive data. A dual top-down and bottom up approach is recommended, combining analysis of documentation and interviews with detection of sensitive data using security controls such as DLP (Data Loss Prevention).
- Classifying PHI so that it may be secured proportional to its sensitivity
- Implementing best practices for procurement, configuration, management and user support
- Tailor applications for use on chosen mobile devices
- Ensure adequate security controls are in place to protect PHI on mobile devices and in the cloud
- Ensuring support across multiple technology platforms, across network topologies (in-house and/or public) and for hospital as well as user-owned devices

Risk Assessment

Healthcare organizations that wish to meet the meaningful use criteria must conduct a risk analysis. The Stage 1 Meaningful Use criteria include the following measure: “Conduct or review a security risk analysis per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.”

Similar requirements for a regular risk analysis exist under the HIPAA security rule, although it does not define a specific method or process for conducting a risk analysis. Therefore, this practice brief will follow the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, “Risk Management Guide for Information Technology Systems.”

---


The scope of risk analysis that the Security Rule encompasses includes the potential risks and vulnerabilities to the confidentiality, availability and integrity of all ePHI that an organization creates, receives, maintains, or transmits. (45 C.F.R. § 164.306(a).) This includes ePHI in all forms of electronic media, such as hard drives, floppy disks, CDs, DVDs, smart cards or other storage devices, personal digital assistants, transmission media, portable electronic media, or mobile devices. Thus, an organization’s risk analysis should take into account all of its ePHI, regardless of the particular electronic medium in which it is created, received, maintained or transmitted or the source or location of its ePHI.

Today’s healthcare providers are facing unprecedented regulatory pressures, government regulations, and legislative policies - all with an increasing sense of urgency and mandated timelines for completion. At the same time, government incentives are stimulating the implementation of increasingly complex Healthcare IT systems. Below is a sample of the regulations healthcare organizations are faced with today, more information regarding up to date regulations can be found on various public websites including The United States Department of Health and Human Services.

HIPAA

  - HIPAA becomes baseline for meaningful use criteria Privacy and Security requirements

HITECH

- HITECH (Health Information Technology for Economic and Clinical Health Act)
  Changes in HIPAA regulations state Business Associates are now responsible to adhere to HIPAA requirements
  - Increased HIPAA penalties with respects to breach disclosures
  - Incentives for Providers to implement electronic medical records as long as they meet meaningful use criteria which includes security and privacy requirements around protected health information (PHI)
  - Increased requirements to notify general public and government agencies of breaches
  - Increased legal exposure associated with noncompliance; risk of criminal and civil law suits

PCI

- PCI - Payment Card Industry
  - Any healthcare provider that accepts credit cards must comply to PCI 2.0 requirements
  - PCI Self Assessment is required

The HIPAA security rule requires covered entities and business associates, their agents, and subcontractors to conduct a risk analysis and implement measures "to sufficiently reduce those risks and vulnerabilities to a reasonable and appropriate level." Specifically, it has three required implementation specifications on risk analysis and risk management:

- "...conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information..." Risk Analysis §164.308(a)(1)(ii)(A)

---

6- http://www.hhs.gov
In summary, HIPAA requires that healthcare providers:

- Perform regular risk assessments
- Address reasonably anticipated risks to Protected Health Information
- Applies to any form of PHI / PII, not just electronic data
- Implement the appropriate administrative, physical and technical safeguards

The HITECH (Health Information Technology for Economic and Clinical Health) Act under the 2009 ARRA (American Recovery and Reinvestment Act) stipulates a number of new compliance rules.

Changes affecting all providers:

- **Enforcement**: The HITECH Act contains language that implies that HIPAA enforcement will be stepped up, for example, HHS is now required to conduct periodic audits of covered entities and business associates. Further, penalties are generally higher and mandatory penalties will be imposed for "willful neglect." Civil penalties can be as high as $250,000, with repeat/uncorrected violations extending up to $1.5 million per incident. Also, States’ Attorney General can now file a law suit.
- **Applicability**: Business Associates (BA) are now required to comply with the safeguards contained in the HIPAA Security Rule. Further, BA’s are now required to report security breaches to covered entities and they are subject to certain civil and criminal penalties under HIPAA.
- **Breach Notification Law**: requires health care providers and other HIPAA covered entities to promptly notify affected individuals of a breach or unauthorized uses and disclosures of "unsecured PHI" (under the HITECH Act "unsecured PHI" essentially means "unencrypted PHI"), as well as inform the HHS Secretary and the media in cases where a breach affects more than 500 individuals. Notification shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery. Breaches affecting fewer than 500 individuals will be reported to the HHS Secretary on an annual basis. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate.

In addition, the following is required to qualify for reimbursements under “Meaningful Use” Stage 1 Core Measures:

- In order to meet Stage 1 Meaningful Use criteria providers are required to perform a regular security risk analysis of and to implement security updates as necessary and correct identified security deficiencies as part of its risk management process. Such security risk analysis should be comprehensive across organizational entities, business associates and partners, and should cover all aspects of integrity, availability, and confidentiality of ePHI.
- Key is that any findings are mitigated and that the analysis is reviewed and repeated on a regular basis.

Additional requirements may be articulated in the subsequent Stages 2 or 3 when those criteria are finalized.
Security

Security and Privacy Controls
Privacy and Security rules apply to a variety of organizations ranging from large integrated delivery systems to small physician practices, as well as their business associates, the standards are flexible in regard to the approach an organization takes based on several factors:

- The organization’s size and complexity
- The organization’s technical infrastructure, hardware, and software security capabilities
- The probability and criticality of potential risks to ePHI
- The organization’s maturity and capability
- The organization’s risk tolerance and limits
- The organization’s business policy and procedures related to PHI and Designated Record Sets

Securing PHI
Protected Health Information (PHI) is in constant motion. Most of the time this information is shared with authorized providers and patients, but often unauthorized individuals attain access to ePHI (Electronic Protected Health Information). The challenge is to secure PHI and ensure that authorized Health Care providers have access to critical data when it is needed.

The risk of a data breach is high for Health Care organizations. In 2010, the average cost per incident of a data breach in the United States was $7.2 million, an increase of 7 percent from 2009. The average cost per loss of a Health Care record is $301. Health Care organizations are ranked as highest likely to have a data loss incident at 30 percent in comparison to all other industry segments. It is likely an unprotected peer you know will experience a data breach.

As information becomes more accessible, ePHI (electronic Protected Health Information) is easily dispersed to various locations. The risk of a data breach increases in proportion to the number of ePHI locations, because more locations mean a larger target area of attack or loss. Across the enterprise, it is likely that you do not have the same levels of security throughout your Health Care’s network storage devices, file servers, endpoint clients or removable storage devices. Also, ePHI dispersion is increasing as Health Care providers are seeing the edge of the network broaden to include mobile devices, virtual deployments and the data going to and from the cloud.

Symantec and Intel Solutions Mapping

PGP Whole Disk Encryption from Symantec™ / Intel® AntiTheft and Advanced Encryption Standard – New Instructions

- PGP Whole Disk Encryption from Symantec™ has been expanded to include support for Intel® Anti-Theft and Intel® Advanced Encryption Standard – New Instructions Technologies. The integration allows customers to protect their devices and their data while helping to deter notebook computer thefts, protect systems during shipping and lower the cost of decommissioning older hardware.
- Intel® Anti-Theft Technology enables network administrators to remotely disable functionality on corporate assets after a theft or loss. Managed by PGP Universal Server from Symantec™, a lost or stolen notebook can be disabled by the administrator, and later reactivated if the system is recovered.
- Intel® Advanced Encryption Standard – New Instructions enables hardware acceleration of encryption and decryption for improved end user experience and compliance. It also drops the core of the encryption and decryption to the hardware layer where it is more resilient to increasingly sophisticated malware, including side channel attacks.
- PGP Whole Disk Encryption from Symantec with Intel® Anti-Theft Technology combines the best attributes of software and hardware into a robust solution, helping to provide businesses mobility with peace of mind.

VeriSign™ Identity Protection / Intel® Identity Protection Technology

- Symantec’s VeriSign™ Identity Protection credential has been integrated into the Intel® Identity Protection Technology found in 2nd Generation Intel® Core processor platforms, including Intel® Core vPro processors.
- By combining VeriSign Identity Protection with Intel® Identity Protection Technology, a new class of strong authentication credential is made available to the enterprise and consumer PC users. This new credential form factor provides a highly secure, easy to use and cost-effective way to implement strong authentication.
- Because the credential is embedded in the Intel chipset, strong authentication within an enterprise environment has now become faster, cheaper and easier to manage. The need to purchase, replace or download credentials is now eliminated, allowing enterprise IT departments

Privacy and Security Risk Assessment

- Single stop for measuring administrative, technical and physical safeguards outlined by HIPAA
- Limited HIPAA/HITECH Act knowledge necessary
- Meets single and multiple provider and location requirements
- Annual assessment data collection and verification
- Automatic assessment and audit log
- Accessible via any web browser
Additional Considerations:

- Cyber security (Symantec™ Endpoint Protection, Symantec™ Critical System Protection)
- Altiris IT Management from Symantec™ with Intel® vPro™ integration (AMT)
- Symantec™ Data Loss Prevention
- General compliance and process management (including risk analysis): Symantec™ Control Compliance Suite, Symantec™ Security Information Manager

References and Further Education


The Office of the National Coordinator for Health Information Technology, “Electronic Health Records and Meaningful Use.”
http://healthit.hhs.gov/portal/server.pt?open=512&objID=2996&mode=2


Product Disclaimers

Intel® Anti-Theft Technology (Intel® AT-p) requires the computer system to have an Intel® AT-enabled chipset, BIOS, firmware release, software and an Intel AT-capable Service Provider/ISV application and service subscription. The detection (triggers), response (actions), and recovery mechanisms only work after the Intel® AT functionality has been activated and configured. No system can provide absolute security under all conditions. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. For more information, visit http://www.intel.com/go/anti-theft

Intel® AES-New Instructions (Intel® AES-NI) requires a computer system with an AES-NI enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on Intel® Core™ i5-600 Desktop Processor Series, Intel® Core™ i7-600 Mobile Processor Series, and Intel® Core™ i5-500 Mobile Processor Series. For availability, consult your reseller or system manufacturer. For more information, see http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/

Intel® Identity Protection Technology: No system can provide absolute security under all conditions. Requires an enabled chipset, BIOS, firmware and software and a website that uses an Intel® IPT Service Provider’s Intel IPT solution. Consult your system manufacturer and
Service Provider for availability and functionality. Intel assumes no liability for lost or stolen data and/or any other damages resulting thereof. For more information, visit http://ipt.intel.com/

Intel® vPro™ Technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software and IT environment. To learn more visit: http://www.intel.com/technology/vpro
About Symantec and Intel

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

Intel (NASDAQ: INTC) is a world leader in computing innovation. The company designs and builds the essential technologies that serve as the foundation for the world’s computing devices. Additional information about Intel is available at newsroom.intel.com and blogs.intel.com.