SOLUTION BRIEF
Hardware-based Security Solutions
Healthcare Information Security

Improving Healthcare Risk Assessments to Maximize Security Budgets

David Houlding, CISSP, CIPP
Healthcare Privacy and Security Lead Architect
Intel Corporation

Tim Casey, CISSP
Senior Information Risk Analyst
Intel Corporation

Matthew Rosenquist
Security Strategist
Intel Corporation

Introduction

Healthcare is undergoing major changes that are being driven by medical, consumer, IT, and security trends. While these trends deliver compelling benefits to healthcare organizations, workers, and patients, they also carry significant privacy and security risks. Healthcare organizations are seeing an escalation in the frequency and impact of security compromises, driving a corresponding increase in healthcare privacy and security regulation at the national and local levels.

In general, the healthcare industry lags behind other industries in IT security. Fortunately cyber crime has not advanced as quickly in healthcare as it has in other industries, such as financial services. This may give the healthcare industry the time it needs to review their privacy and security policies to prevent the potentially devastating business impacts of security breaches and cyber crime.

This paper looks at how healthcare organizations can better optimize and focus their privacy and security efforts and budgets through risk assessments designed to identify, characterize, and address the most serious threats and the agents behind them.

Keeping the Focus on Patient Care

The impact of security incidents such as breaches on healthcare organizations is relatively well understood. Progressive healthcare organizations are increasingly recognizing the seriousness of security breaches involving sensitive patient information. This is especially true with connected medical devices where security incidents can go beyond financial and psychological harm, affecting the availability and integrity of sensitive healthcare information and presenting direct threats to patient safety.

TRENDS DRIVING PRIVACY AND SECURITY RISKS

Medical Trends

- Electronic Health Records
- Health Information Exchange and data proliferation
- Mobile health
- Care coordination
- Connected medical devices
- Regulation complexity, breach notification
- Cost reduction pressure

Consumer Trends

- Consumerization of mobile devices[1]
- Social media and social engineering

IT and Security Trends

- Cloud computing and virtualization
- Patching, application proliferation
- Monoculture of platforms and formats
- Threat sophistication: targeted or covert

A fundamental limitation to healthcare organizations in improving their security posture is the available resources, and in particular, budget. The healthcare industry is under great pressure to reduce costs, and this restricts the money available for privacy and security measures. In addition, privacy and security, while recognized as important, are not the primary goals of healthcare. The number one priority is great patient care.

Given these challenges, healthcare organizations must put the limited funds available to the best use to optimize the privacy and security of patient information. Because this can lead to over-securing some areas and leaving others more vulnerable, preparing risk assessments helps the industry prioritize their spending more appropriately.

Saving Money through Risk Assessments

Risk assessments are a best practice that can help direct limited budget dollars in a prioritized and measured way that reduces the most business risk. Simply defined, a risk assessment is the identification, evaluation, and estimation of risks, including a determination of the baseline acceptable level of risk.

Recent evidence shows that the healthcare industry needs to make better use of risk assessments. A 2011 analysis on healthcare organization breaches reports a 97-percent increase in total records breached in 2010–2011.[2] The report's authors noted that "it is strikingly clear that woefully inadequate security risk analysis (if any) took place prior to the occurrence of these incidents. A proper risk-based assessment would have identified and brought attention to these large concentrations of PHI [protected health information] and raised the issue of whether sufficient security controls were in place ... "[3]

Risk assessments also enable a measured approach to privacy and security that keep them from becoming a budgetary black hole.

Risk Assessments Save Healthcare Organizations Money

Risk assessments can help provide direction to privacy and security efforts and save money for healthcare organizations.

- **Focus on real risks.** Proactive risk assessments based on accurate, objective, comprehensive, and current information about real healthcare security threats can replace fear, uncertainty, and doubt with clarity and focus.
- **Prioritize risks.** By identifying the most probable and potentially damaging risks, risk assessments help guide the allocation of limited resources toward addressing the risks that are most likely and have the largest business impact first.
- **Proportionally allocate resources.** This approach to risk assessments allocates resources to safeguards proportional to the value and sensitivity of the healthcare data at risk. Data that is more sensitive and valuable get more resources, stronger safeguards, and a great number of safeguards in a defense-in-depth approach.
- **Layer defenses over time.** Regular risk assessments performed at least annually and at key milestones can provide valuable insight on how best to allocate the budget to building up layered defenses.
- **Avoid budgetary black holes.** In risk assessments, a baseline of acceptable risk helps provide an achievable target for mitigating risk, avoiding the use of too much security in some areas and not enough in others.
- **Implement regulatory incentives and penalties.** Performing and documenting risk assessments, as well as the steps taken to address any deficiencies in identified safeguards, help satisfy meaningful use requirements for qualifying for financial incentives.

Focus on Real Risks

With all the sensational news about privacy, security issues, and breaches, it is easy to be swayed by public perception and to respond to cyber threats in panic—especially if faced with a real security incident in the organization.[4] Panic-driven reaction is counterproductive, if it results in inefficient resource allocation when addressing the threat.

Proactive risk assessments based on accurate, objective, comprehensive and current information about real healthcare security threats can replace fear, uncertainty, and doubt with clarity and focus. For instance, seemingly mundane risks such as curious workers looking through colleagues' sensitive healthcare data can often be a much greater portion of the real risks facing a healthcare organization than the dramatic but unrelated risks from outside agents featured in the media. In fact, the business impact from risks driven by internal agents is poised to grow with proposed new rules that grant patients the right to see who has electronically accessed their protected health information.[5] A proactive healthcare organization using risk assessment methodologies can better evaluate and determine the real risks facing the organization and can manage these risks down to acceptable levels.

Prioritize Risks

Given the fundamental constraint of limited resources and recognizing that an organization can't eliminate every possible risk, risk assessments provide a methodical way to evaluate and prioritize risks. By identifying the most probable and potentially damaging risks, risk assessments help guide the allocation of limited resources toward addressing the risks that are most likely and have the largest business impact first.

Proportionally Allocate Resources

Risk assessments performed with an awareness of the value of sensitive healthcare data can help healthcare organizations mitigate risks with the appropriate level of security. By understanding how motivated various threat agents are, an organization can more precisely determine the strength and number of safeguards needed to reduce the risk to an acceptable level. In many cases, the motivations may be so strong, and risks so high, that a defense-in-depth approach is required. This type of approach uses multiple layers of security controls to provide redundancy in case a security control fails or vulnerability is exploited.

More can be learned about the types of healthcare data and their value to cyber criminals through the RSA white paper "Cybercrime and the Healthcare Industry."[6]

Layer Defenses over Time

As a general rule, any safeguard has residual risk. For example, even strong encryption is vulnerable to users who choose weak passwords or share them. We can mitigate residual risk with a layered or defense-in-depth approach built up iteratively over time as available resources permit.[7]

Regular risk assessments performed at least annually and at key milestones can provide valuable insight on how best to allocate the budget to building up layered defenses. Taking the latest trends and risks into consideration in each iteration of the risk assessment provides a way to track the fast-evolving threat landscape and ensure adequate privacy and security over the long term.

Avoid Budgetary Black Holes

In a reactive approach to protecting privacy and security, it is difficult to tell when the measures are good enough. Given the general rule that no safeguard is free of residual risk and that an organization can continue to reduce residual risk through successive layers of safeguards, the question becomes: When is the protection good enough? This situation is analogous to performance optimization where one can keep applying improvements to get increased system performance but at some point faces diminishing returns because of the cost and the effort. In performance optimization, a target performance threshold helps answer

Given the general rule that no safeguard is free of residual risk and that an organization can continue to reduce residual risk through successive layers of safeguards, the question becomes: When is the protection good enough?

Table 1. A brainstorming list of potential healthcare threat agents

- Healthcare Rights Activist
- Reckless Healthcare Worker
- Curious Healthcare Worker
- Distracted Healthcare Worker
- Untrained Healthcare Worker
- Prescription Fraudster
- Medical Claims Fraudster
- Financial Fraudster
- Disgruntled Healthcare Worker
- Business Associate
- Irrational Individual
- Thief
- Cyber Vandal
- Competitor
- Legal Adversary
- Vendor
- Research Lab Activist
- Radical Activist
- Sensationalist

For Intel internal risk assessments, a threat agent is defined as a person who, for personal, monetary, or other reasons, seeks to obtain or compromise information for an unauthorized purpose.

this question. In risk assessments, a baseline of acceptable risk helps provide an achievable target for mitigating risk, avoiding the use of too much security in some areas and not enough in others. Once the highest priority risks are mitigated to a point where the residual risk is below the baseline of acceptable risk, the current cycle of risk assessment and security iteration is considered complete. This approach to risk assessments allocates resources to safeguards proportional to the value and sensitivity of the healthcare data at risk. More sensitive and valuable healthcare data gets more resources, stronger safeguards, and a great number of safeguards in a defense-in-depth approach.

Implement Regulatory Incentives and Penalties

Regulatory incentives, such as those provided by the U.S. federal government for the meaningful use of health information technology, include core objectives for securing sensitive healthcare data. Performing and documenting risk assessments, as well as the steps taken to address any deficiencies in identified safeguards, help satisfy meaningful use requirements for qualifying for financial incentives. They are also key aspects of regulatory compliance and the avoidance of potential regulatory penalties in an audit or in the event of a breach.

The U.S. Department of Health & Human Services performs periodic audits to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security rules and Breach Notification Standards. These audits are conducted by the Office of Civil Rights.[8] The HIPAA Security Rule includes requirements for risk management, requiring a healthcare-covered entity to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronically protected health information held by that entity.[9] Similar healthcare regulations protecting the confidentiality, integrity, and availability of sensitive healthcare data appear at both national and local levels globally.

Types of Risk Assessments

The simplest type of risk assessment suitable for most healthcare organizations, is the qualitative risk assessment. It assigns qualitative measures—such as high, medium, or low—to the probability of occurrence and business impacts of each risk.

Quantitative risk assessments are seemingly more precise, but are much more difficult to perform. For example, attempting to assign a monetary value to the business impact of damage to a healthcare organization's reputation resulting from a breach can be a complicated and an inexact science. It can result in the risk assessment process itself becoming time-consuming and expensive.

Keeping risk assessments simple avoids exorbitant time expenditures and costs. To complement this strategy, after a qualitative risk assessment has identified the highest priority risks, a targeted return on investment (ROI) analysis can be done on select highest priority risks.[10] This can help motivate financial stakeholders to implement recommended safeguards to improve the security posture of the organization.

Healthcare Threat Agents

In business, sports, and politics, people focus on the strengths, weaknesses, and methods of opponents in order to allocate limited resources in ways that maximize one's chance of achieving goals. However, in healthcare, risk assessments are often centered on vulnerabilities, not the threat agents associated with various risks.

For Intel internal risk assessments, a threat agent is defined as a person who, for personal, monetary, or other reasons, seeks to obtain or compromise information for an unauthorized purpose. Threat agents represent a wide spectrum of people, motives, methods of access, and potential damages to an organization's information and systems (see Table 1). For example, a threat agent might be an insider, such as a Curious Healthcare Worker looking at the sensitive healthcare records of a colleague or patient. Or a threat agent might be external, such as a Prescription Fraudster.

There are, of course, non-human information security threats as well. These include natural and environmental threats, such as earthquakes, power loss, and flooding. However, because human threats often account for the majority of risks in a healthcare organization, this paper focuses on human threat agents.

Because threat agents lack standard definitions, threat information has been historically fragmented and sensationalized in almost every industry. For example, the term *hacker* describes anyone who intrudes into computer systems for any purpose. However, it provides little insight into the person an organization needs to defend against and how. With no clear definition of the threat agents an organization faces, risk assessments lack focus and direction, and can become full of hypothetical distractions that divert attention from real risks, resulting in misdirected and over-budget security and privacy plans that try to accomplish more than is really necessary or justified.

The Threat Agent Library

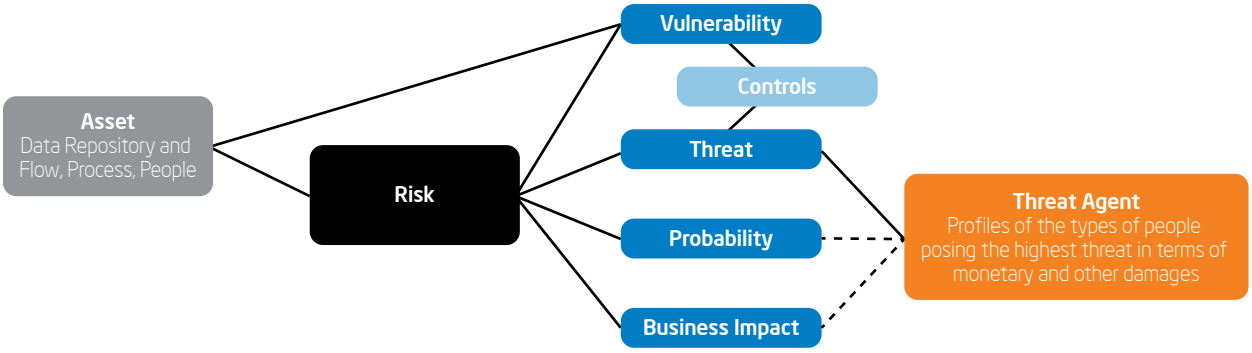
To enable an organization to more quickly and precisely assess risks from specific agents and devise security strategies to mitigate these risks, Intel has developed a coherent system for creating and assembling a comprehensive set of archetypal agent definitions into a threat agent library (TAL).

Figure 1 shows the factors taken into consideration when creating a threat agent profile. By determining for each agent the nature of the threat posed, the probability of a compromise, and the potential business impact, an organization can more strategically invest in appropriate controls for the risk and vulnerability of each asset. All threat agent profiles are stored in the TAL and become an integral part of risk assessments. The U.S. Department of Homeland Security incorporates Intel's TAL approach as part of its IT Sector Baseline Risk Assessment to identify and prioritize national-level risks to critical, sector-wide IT functions while outlining strategies to mitigate those risks and enhance national and economic security.[11]

A TAL is created by an organization's privacy and security team. It involves researching potential agents and their recent activity, then creating a set of archetypes based on the threat agents deemed most significant. The privacy and security team then uses the TAL to:

- Provide a common and repeatable reference point for risk assessment
- Guide the development and prioritization of security and privacy safeguards focused on specific threat agents and their targets
- Act as a collection point for multiple and disjointed threat information sources, making it easier to categorize, analyze, and share that information

Figure 1. Creating threat agent profiles for a threat agent library.



Once the threat agent list is complete, character sketches are created of each agent to help understand their motivations and how they might breach security or privacy safeguards.

Creating a Threat Agent Library

Building a library of agents is straightforward, with the greatest time commitment spent in the initial effort. Designers of a TAL start by developing a common set of attributes—a taxonomy—that can be used to define each agent uniquely. For example, intent might be one common attribute and agents could be categorized against this attribute as either hostile or non-hostile. A hostile agent starts with the intent to harm or use assets inappropriately. A non-hostile agent starts with good intentions but may mistakenly or accidentally perform actions that harm assets such as sensitive healthcare data. Other ways of categorizing agents include whether they're internal or external, the motives or outcomes of their actions, their skills in breaking into computer systems, and their objectives—such as to deny service, steal files, or destroy data.

The next step is to develop a list of all potential threat agents, as shown in Table 1.

Once the list of potential threat agents is completed, it is culled by removing those that represent only a marginal risk. For example, Research Lab Activist and Healthcare Rights Activist might be eliminated after deciding that Radical Activists are a superset of all the activist threat agents that could impact patient care. Agent categories can be combined as well if there is little functional difference between them. For example, Medical Claims Fraudster and Financial Fraudster might be assigned a single entry: Fraudster.

Among healthcare organizations, TALs will have significant overlap. For instance, nearly all healthcare organizations have to be on guard for Disgruntled Healthcare Workers because it is well-known that unhappy workers in any organization can compromise the integrity of information systems. Networked healthcare organizations can achieve considerable savings by using the same library and adjusting for any local, organizational, or other differences, so local threats can be contained.

Once the threat agent list is complete, character sketches are created of each agent to help understand their motivations and how they might breach security or privacy safeguards. For example, a character sketch for Fraudsters might describe them as: Individuals interested in the unauthorized use of healthcare records for personal financial gain, either through prescription fraud, medical claims fraud, or financial fraud. May or may not have authorization to view records.

After the character sketches are completed, each character's specific attributes are determined from the taxonomy created earlier. This step requires extensive consideration and discussion, and is quite iterative. While defining each individual character is straightforward, it is common to discover inconsistencies or overlaps in characters when comparing them to each other. On the positive side, working through these details compels a team to sort through facts and hype to more clearly determine the actual threats each agent represents and to develop a common, team-wide understanding of them.

The final step is to publish each agent description in an easily accessible file. The more extensive threat agent descriptions help risk assessors and managers fully understand and link the threat agents to each risk in a risk assessment. Extended descriptions provide a full sketch of the agent in narrative form, including typical actions, motivations, methods, and any other information that help others understand each agent and its associated threats. Organization-specific information, such as examples of actual security assessments or incidents, is also helpful.

Once complete, these files must be properly managed and updated to track the continually evolving threats, threat agents, and landscape. This ensures the TAL continues to provide valuable information for risk assessment and the development of appropriate security solutions.

Table 2 is an example of a TAL for the healthcare industry.[12] Coming from an original Intel TAL, the taxonomy used for this example is suitable and available for use in the healthcare domain.

Table 2. Example of a threat agent library for the healthcare industry

		THREAT AGENTS NON-HOSTILE INTENT				THREAT AGENTS HOSTILE INTENT							
THREAT AGENT ATTRIBUTES		Reckless Healthcare Worker	Distracted Healthcare Worker	Untrained Healthcare Worker	Business Associate	Fraudster	Healthcare Data Thief	Disgruntled Healthcare Worker	Vendor	Radical Activist	Cyber Vandal	Irrational Individual	Curious Healthcare Worker
Access	Internal	■	■	■	■		■	■	■				■
	External					■	■			■	■	■	
Outcome	Acquisition/Theft					■	■						■
	Business Advantage								■				
	Damage	■	■	■	■			■		■	■	■	
	Embarrassment	■	■	■	■			■		■		■	
	Tech Advantage								■				
Limits	Code of Conduct		■	■	■								■
	Legal	■				■	■		■				
	Extra-legal, minor									■	■		
	Extra-legal, major							■				■	
Resources	Individual	■	■	■	■		■	■				■	■
	Club												
	Contest										■		
	Team								■				
	Organization					■				■			
	Government												
Skills	None											■	
	Minimal			■									
	Operational		■		■		■	■	■		■		
	Adept	■				■				■			■
Objective	Copy								■				■
	Deny												
	Destroy							■					
	Damage							■					
	Take					■	■						
	All of the above/Don't Care	■	■	■	■					■	■	■	
Visibility	Overt		■	■						■			
	Covert	■				■	■				■		■
	Clandestine				■				■				
	Multiple/Don't care							■				■	

Note: Healthcare organizations can use this table to develop their own threat agent library, adapting it to their particular risk environment.

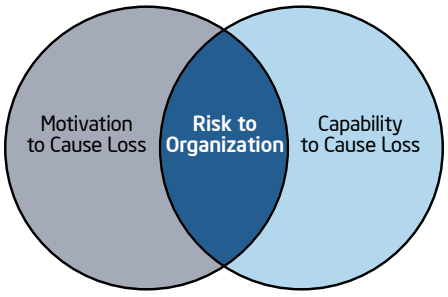
Determining Who to Target

As noted earlier, nearly all privacy and security breaches originate with people. Threat agents write viruses, embezzle funds, mine data, mischievously hack into systems, and make unintentional errors—all of which result in loss for the organization. Threat agents may be strangers or trusted employees. They can be brilliant, agile, and opportunistic. Or, they can be simply sloppy or forgetful. Threat agents and the risks they present abound everywhere—making it hard to predict the time or place of attacks.

Building a TAL helps distill the immense number of possible time windows and sources of attacks down to a list of the most likely agents to cause losses. Focus on the agents that fall in the intersection between people motivated to cause loss and the people capable of doing so, as shown in Figure 2. People outside this intersection represent a community of much lower risk.

Understanding the motivations and capabilities in the high-risk overlap provides insights to the likely methods threat agents employ to achieve their objectives. Armed with specific information on these methods, predictive decisions can be made on how best to disrupt likely attacks through prevention, detection, and response measures.

Figure 2. Organizational risk from threat agents.



Plugging the Holes

In general, hostile threat agents are tied to their objectives and tend to use a standard set of breach methods. Understanding each type of attacker helps provide a better picture of what they will attempt and how they will go about it, giving the organization a predictive advantage. To save time, organizations can start by crossing off any method where sufficient controls are already maintained to mitigate the risk. These breach methods won't require any further research.

The best way to understand an attacker is for team members to put themselves in the shoes of each potential threat agent. In healthcare security, this might mean assuming the mindset of an impersonating fraudster, seeking to copy patients' sensitive healthcare data—such as the PHI used by healthcare clearinghouses, health plans, and medical service providers—by compromising the online registration database.

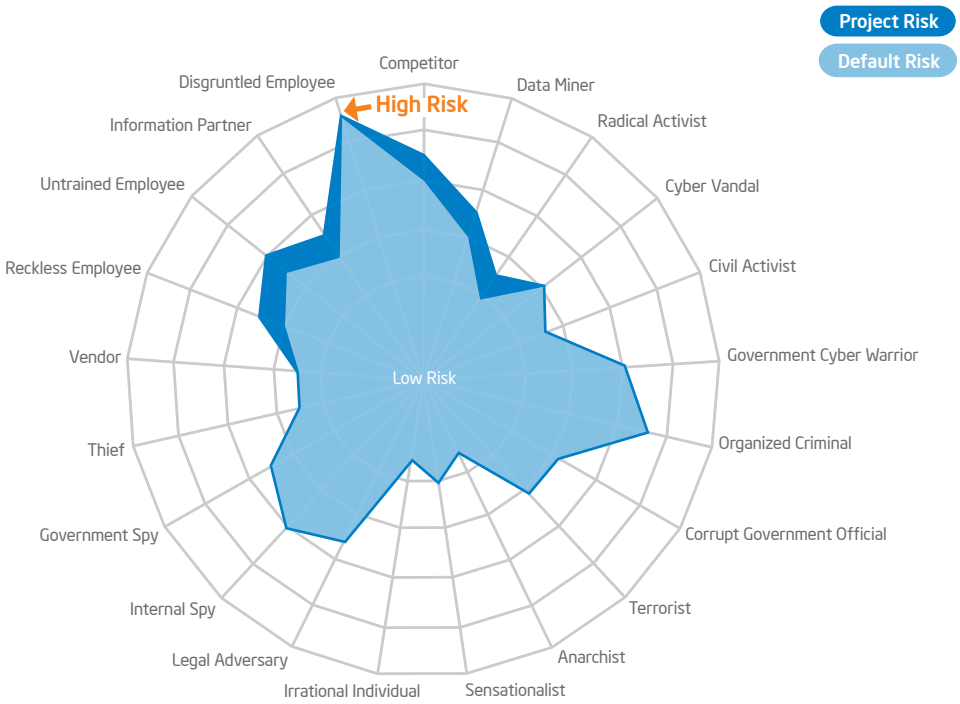
It is also important to understand the value of the healthcare data to the threat agents to predict how much effort they will put into obtaining the data and how strong the safeguards—or how deep the defense-in-depth approach—need to be. The World Privacy Forum, for instance, has reported that the street cost for stolen medical information is USD 50, versus USD 1 for a stolen Social Security number.[13] The average payout for a medical identity theft is USD 20,000, compared to USD 2,000 for a regular identity theft.[14]

Threat Agent Risk Assessment

One of the best ways to accomplish risk assessment is through the Threat Agent Risk Assessment (TARA) approach. Developed by Intel, this methodology helps identify the most likely attack vectors and the optimal security strategies for them.[15]

A new direction in information security risk assessment, TARA methodology is substantially different from vulnerability assessments that attempt to identify every single weak point. By narrowing the number of threat vectors to those most likely to occur, TARA reduces the threat surface that must be protected and communicates this information in an easy-to-understand format, as shown in Figure 3.

Figure 3. The threat agent risk assessment methodology provides information necessary to highlight the difference in risks of specific threat agents to a project, in comparison to default risks which already exist. Insights allow for these areas to be the focus of the follow-on analysis.



Through TARA, organizations have a straightforward procedure for classifying a threat agent's motivations, capabilities, and objectives, and can map them to likely breach methods, as shown in Figure 4. Each time a likely method intersects a vulnerability without controls, it uncovers an area of exposure. Taking impacts into consideration, these resulting exposures represent the most critical and high-priority areas of concern.

TARA makes it easier to adjust to changes in threat agents, attack methods, and attacker objectives. In fact, its predictive results can be validated over time to help better manage and allocate resources against risks. TARA's reusable indexes of threat agents, methods and objectives, and the vulnerabilities specific to an organization, facilitate rapid repeatability and reassessment. Outputs show the changes in relative risks over time and can be overlaid with boundaries of what an organization considers acceptable risk. Such metrics make it easier to justify the choice of resources used to manage specific threats that exceed thresholds.

Ensuring Risk Assessments Are Implemented

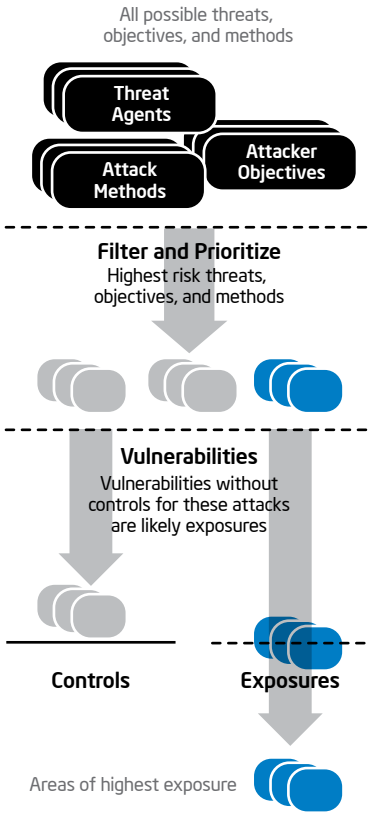
Being able to predict the most likely and impactful risks is a tremendous advantage, which is why good risk assessments are an integral part of a robust privacy and security practice in a healthcare organization. They feed the prediction elements, helping organizations avoid hypothetical risk distractions and establish the optimal strategy for the prevention, detection, and response areas for the most likely and serious threats.

However, risk assessments don't directly improve the security posture of a healthcare organization; acting on the safeguard prescriptions identified by the risk assessments does. All too often a busy staff may casually waive a specific safeguard that a risk assessment prescribes. For example, an IT manager with scarce time, budget and resources, as well as a long to-do list, may delay implementing an important safeguard, such as data encryption. For this reason, it can help to have a good audit and sign off framework around risk assessments. Such a framework makes it mandatory to have an explicit, formal, and documented sign off, by the individual responsible for implementing the safeguard, in order to waive a risk assessment prescription. Such a waiver can require accepting the liability associated with the risk, motivating the individual to reconsider whether they want to waive or move up the priority of implementing the safeguard.

An ROI analysis for specific high-priority risks, and associated safeguard prescriptions, can help inform and motivate positive decisions by financial stakeholders within the healthcare organization, and improve follow-through on implementing prescribed safeguards. There are a variety of methods for calculating ROI.[16] Putting safeguards in place that mitigate the highest priority risks identified in the risk assessment, and offer the greatest ROI, help improve the security posture of a healthcare organization in a systematic fashion at a reasonable cost.

User acceptance of a new safeguard is critical to its successful implementation. This can depend greatly on the user experience, which in turn depends on good performance of the safeguard. Intel hardware-assisted security technologies provide hardware acceleration of technical safeguards, while also hardening them against increasingly sophisticated malware.[17] Running a pilot or proof of concept on a small target user group also helps enable a great and safe user experience and helps improve user acceptance.

Figure 4. The threat agent risk assessment methodology narrows down the field of all possible attacks to determine the most likely ones.



THREAT AGENT RISK ASSESSMENT (TARA) METHODOLOGY

If you are conducting a simple vulnerability-centric qualitative risk assessment, augment your approach with threat agent awareness, Option A. Once the team sees the value of this approach, progress to the threat agent-centric approach, Option B.

TARA Option A: Threat Agent Aware Risk Assessment

This approach involves conducting a traditional healthcare risk assessment—for example, a qualitative risk assessment—but with awareness of threat agents to improve the value of the risk assessment in focusing on real risks. This avoids hypothetical distractions and identifies the most beneficial safeguards to mitigate risk.

1. Identify sensitive healthcare data repositories, and flows or assets.
2. Identify vulnerabilities and threats for each asset.
3. Identify likely threat agent(s) that are motivated and have the capability to exploit each vulnerability.
4. Assign a probability of occurrence and business impact to each risk, taking into consideration threat agent characteristics.
5. Prioritize risks across threat agents to filter out unlikely threat vectors and methods.
6. For each of the highest priority risks that exceed acceptable risk baselines, identify threat agent methods and safeguards that best block these methods to effectively mitigate risk.

TARA Option B: Threat Agent-Centric Risk Assessment

This approach offers the same benefits as Option A, but starts with the threat agents relevant to the healthcare organization. This approach avoids modeling risks that, while based on real vulnerabilities, aren't a likely target for threat agents and are therefore hypothetical distractions that can blur the focus on real risks.

1. Identify threat agents that represent significant risks to the healthcare organization.
2. Identify sensitive healthcare data repositories, and flows or assets at risk from these threat agents.
3. Using threat agent methods of attack, identify threats to, and vulnerabilities of, these assets.
4. Assign a probability of occurrence and business impact to each risk, taking into consideration threat agent characteristics.
5. Prioritize risks across threat agents to filter out unlikely threat vectors and methods.
6. For each of the highest priority risks that exceed acceptable risk baselines, identify safeguards that best block threat agent methods to effectively mitigate risk.

Conclusion

The healthcare industry is in the midst of major change as more of its systems and data are electronically accessed, stored, and networked. While these changes offer compelling productivity benefits, they also pose significant privacy and security risks. The likelihood of security incidents is increasing and so is the potential business impact of each event, driven by increasing regulation and breach notification rules. In order to safely embrace these changes, the industry needs to implement security best practices and standards, such as ISO/IEC 2700x series.[18]

These concerns come at a challenging time for healthcare organizations. Facing the pressure of major cost reductions, these organizations need ways to make the most of their security budgets in mitigating these new risks.[19]

In this paper, we have examined the use of and value of risk assessments, explaining how when done well, they become a valuable tool and best practice for allocating limited budgets in a prioritized and measured way. Using risk assessments to guide security measure implementation can help reduce the most serious business risks, while helping to keep privacy and security from becoming a budgetary black hole. This paper recommends several techniques to improve and refine risk assessments, including the use of a TAL and a TARA approach. Adding these practical methodologies to a risk assessment program helps maximize the value of risk assessments, providing an efficient discovery process for determining which agents pose the greatest threat.

By implementing better risk assessment methodologies, healthcare organizations will find it easier to adapt to the constantly changing landscape of threat agents and their objectives and methods. This, in turn, enables healthcare organizations to continually make better decisions on how to manage information security risks and properly allocate their limited resources. The end result is a systematic approach to effectively improving the security posture of a healthcare organization at a reasonable cost.

For more information on IT best practices for healthcare, see:
http://premierit.intel.com/community/ipip/healthcare

[1] For more information on the security risks of mobile healthcare devices, see the white paper, "Healthcare Information at Risk: The Consumerization of Mobile Devices" at: http://premierit.intel.com/servlet/JiveServlet/previewBody/6458-102-1-9628/Healthcare%20Information%20at%20Risk%20-%20The%20Consumerization%20of%20Mobile%20Devices.pdf.

[2] "Breach Report 2011: Protected Health Information," Redspin white paper. To access this report, go to: www.redspin.com/resources/whitepapers-datasheets/request_PHI_Breach_Analysis.php.

[3] Ibid.

[4] For an interesting discussion of how perception can drive panic, watch a video of a presentation by computer security expert Bruce Schneier at: www.ted.com/talks/lang/en/bruce_schneier.html.

[5] See www.hhs.gov/news/press/2011pres/05/20110531c.html.

[6] See www.healthcareinfosecurity.com/whitepapers.php?wp_id=338.

[7] For more on why a depth-in-defense approach is often necessary, see the white paper, "Healthcare Information at Risk – Encryption Is Not a Panacea," at: http://premierit.intel.com/servlet/JiveServlet/previewBody/6367-102-1-9576/Healthcare_Information_Risk-Encryption_is_Not_a_Panacea.pdf.

[8] For more on privacy and security audits by the Office of Civil Rights, see: www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html.

[9] For the six basics of HIPAA risk analysis and risk management, see: www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf.

[10] See how risk analysis can demonstrate ROI for security measures. Read the "Intel® Anti-Theft Laptop Risk Tool for Healthcare Information Technology" at: www.intel.com/communities/ipip/anti-theft/launch.htm.

[11] See www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf.

[12] The basis for the agents listed in Table 2 came from an Intel TAL that is available for use without license. Healthcare organizations can use this TAL, together with the sample list of healthcare-specific threat agents in Table 1, as a start to their own library. For more information health organizations can use to create a TAL, see the white paper, "Threat Agent Library Helps Identify Information Security Risks" at: http://communities.intel.com/docs/DOC-1151.

[13] "Cybercrime and the Healthcare Industry," RSA white Paper, www.rsa.com/products/consumer/whitepapers/11030_CYBHC_WP_0710.pdf.

[14] Ibid.

[15] Learn more about TARA through the Intel white paper, "Prioritizing Information Security Risks with Threat Agent Risk Assessment," at: http://download.intel.com/it/pdf/Prioritizing_Info_Security_Risks_with_TARA.pdf.

[16] See "Return on Security Investment (ROSI): A Practical Quantitative Model" by Wes Sonnenreich for one method of determining ROI on security measures at: www.infosecwriters.com/text_resources/pdf/ROSI-Practical_Model.pdf.

[17] Learn more about Intel hardware-assisted security technologies at: www.intel.com/content/www/us/en/enterprise-security/raise-pc-security-with-intel-core-vpro-processors.html.

[18] For information on these requirements, see: www.iso.org/iso/catalogue_detail?csnumber=42103.

[19] See "Healthcare Information at Risk: Successful Strategies for Healthcare Security and Privacy," at: http://premierit.intel.com/servlet/JiveServlet/download/6242-1-6046/Successful%2520Strategies%2520for%2520Healthcare%2520Security_Privacy.pdf.

Printed in USA 0312/DHOU/KC/LP/250 ♻ Please Recycle 326414-001US