HIPAA-Watch for Security™ Speeds Up Compliance
By Laura Taylor
July 26, 2004

Executive Summary

HIPAA-Watch for Security™ is a tool designed to guide organizations through the risk analysis required by the Health Insurance Portability and Accountability Act (HIPAA) compliance process. Relevant Technologies, a leading security research and advisory firm, evaluated HIPAA-Watch for Security™ to verify how well it performed in guiding organizations through the HIPAA security risk analysis process.

Vendor Background and Information

RiskWatch was founded in 1993 in Landover, Maryland with the idea of automating risk assessment modeling for the Department of Defense. Founder, Caroline Hamilton, a statistical modeling expert, put together a prototype for a risk analysis tool and then managed its development into an innovative risk analysis product which was adopted initially by NASA and then the U.S. Patent and Trademark Office.

The original product grew into a full featured product line, and today, HIPAA-Watch for Security™ (HIPAA-Watch) is just one of seven products in the suite of risk analysis tools offered by RiskWatch. In the last three years, and the aftermath of 9/11, RiskWatch has seen unprecedented growth and has expanded into international markets. RiskWatch anticipates that their biggest growth in the near term will be in HIPAA and financial compliance (Sarbanes Oxley and Gramm-Leach-Bliley). RiskWatch is actively looking for qualified investors who share the vision of becoming a world leader in risk analysis. Without new investment capital, Relevant Technologies expects that RiskWatch could become a potential acquisition target by a larger information security monolith.

Table 1. Company Information

<table>
<thead>
<tr>
<th>Company Name</th>
<th>RiskWatch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employees</td>
<td>14</td>
</tr>
<tr>
<td>Headquarters</td>
<td>2568A Riva Road, Suite 300, Annapolis, MD, 21401</td>
</tr>
<tr>
<td>Product Name</td>
<td>HIPAA-Watch for Security™</td>
</tr>
<tr>
<td>Key Features</td>
<td>NIST 800-26 compliant, Automatic Reporting, Auditing, Multi-User Response System, Life-Cycle Management, Automated Financial Calculations: Annual Loss Expectancy, Cost Benefit Analysis, Return on Investment; Customizable</td>
</tr>
<tr>
<td>Company URL</td>
<td><a href="http://www.riskwatch.com">http://www.riskwatch.com</a></td>
</tr>
<tr>
<td>Product URL</td>
<td><a href="http://www.riskwatch.com/hipaa.asp">http://www.riskwatch.com/hipaa.asp</a></td>
</tr>
<tr>
<td>Customer Contact</td>
<td>800-448-4666</td>
</tr>
<tr>
<td>Investor Inquiries</td>
<td><a href="mailto:invest@riskwatch.com">invest@riskwatch.com</a></td>
</tr>
</tbody>
</table>
**HIPAA Regulation and Compliance Requirements**

HIPAA was signed into law by President Clinton on August 21, 1996 and authorized the Secretary of Health and Human Services to provide Congress mandatory regulations to secure and protect the privacy of patient medical records. The primary purpose of HIPAA was to ensure that patient medical records are kept private and are not exploited. However, the impact of keeping patient records private has been to secure the information technology infrastructure that serves as the steward of patient medical records. Securing the information technology infrastructure is the means to the end for securing the data.

Securing information technology systems, and the physical components that surround them, is anything but simple. There are endless factors that need to be taken into consideration when securing infrastructure, and thanks to HIPAA, non-compliance is a crime with severe penalties including possible fines and prison sentences. HIPAA compliance requires organizations to converge law, technology, and medical information into an understandable mélange of sensibility.

HIPAA-Watch for Security™ is an effort to guide organizations through the security risk analysis and down the road to compliance, through a carefully thought-out risk methodology based on a survey approach. I tested out HIPAA-Watch after spending considerable time thinking about all the manual ways to comply with HIPAA while authoring three chapters of *HIPAA Security Implementation* (SANS, ISBN 0-9743727-2-2) including the chapter on risk analysis. Clearly a software tool is not a replacement for reference books and true understanding, however, if you’re crunched for time, and you don’t know where to start, what I found is that HIPAA-Watch for Security™ will jump-start your project and navigate you through a sea of intricate details.

**Using HIPAA-Watch for Security™**

HIPAA-Watch for Security™ is based on RiskWatch's core risk analysis engine that is embedded in all their products and is currently released at version 9.2, which was released in June 2004. The embedded risk analysis engine guides you logically through four phases of HIPAA compliance enabling you to go back and make corrections, changes, and updates as necessary. The four phases that HIPAA-Watch for Security™ leads you through consist of the following:

- Phase I: definition
- Phase II: data
- Phase III: evaluation
- Phase IV: reports.

Phase I assists you in setting up your compliance case boundaries. If you are a large health care organization, it is likely that you may want to create multiple cases. HIPAA-Watch gives you the ability to create as many new cases as necessary. During Phase I, you define Functional Areas, Asset Categories, Loss Categories, Threats, Vulnerability Areas, and Safeguards.

Phase I helps you understand what is at risk, what the potential disasters are waiting to occur, and what impact those disasters could have on your organization. Phase I also prompts you to define and analyze your potential losses, vulnerabilities, threats, and safeguards, including how widely they are implemented in the organization.
In Phase II, the assets that need to be protected are selected and valued, including values for how much the organization depends on each asset; and the likelihood of a threat occurrence is integrated into the assessment. HIPAA Watch for Security™ presents you with default values for threat frequencies based on Local Annual Frequency Estimates (LAFE) and Standard Annual Frequency Estimates. The LAFE value should be a function of your local information such as penetration test data and incident report data, and during phase II, you have the opportunity to modify the LAFE value or use the standard defaults that are built into the product. For example, if your organizational assets are in Kansas City there is a much greater LAFE value for a tornado in Kansas City, Kansas than there would be for Portland, Maine since tornados are much more likely to occur in Kansas City.

During Phase II you can indicate what percentage of the identified potential and existing safeguards have been implemented which is a key feature to take into consideration for life-cycle management and project management. At any given time, it is unlikely that all your safeguards are either completely implemented or not. You might have a security policy that is 75% completed, a firewall that just entered the procurement phase, and an intrusion detection system that has been implemented at 6 out of 10 locations. You cannot accurately calculate a viable risk analysis without accurately indicating the percentage of implementation that has been completed for each safeguard, and HIPAA-Watch allows you to indicate projects that are not fully implemented as illustrated in Figure 1.

Phase II also encompasses setting up a survey of audit questions and setting up the different respondents (by job category) who are best apt to be able to answer these questions, illustrated in Figure 2. You can setup as many respondents as necessary and assign particular questions to these individuals based on their area of expertise which have been designated Functional Areas. As elsewhere in HIPAA-Watch, these categories can be modified, deleted, or you can add your own job categories. The current Functional Areas that come bundled with HIPAA-Watch for Security™ include:
• Admissions / Patient Intake
• Billing / Collections
• Business Associates
• Case Management / Disease Management
• Claims Processing
• Compliance / Legal Office
• Facilities Management
• Financial Management and Budget
• Health Education
• Health Services / Utilization Management
• Human Resources
• Information Network Management
• Information Security Officer
• Information Services Help Desk / Technical Support
• Information Systems Management
• Internal Audit
• Laboratory
• Marketing and Fund Raising
• Medical Records Department
• Medical Staff
• Member / Customer / Patient Services
• Mental Health / Drug Alcohol
• Operations Department
• Patient / Member Communication
• Patient / Member Medical Records
• Pharmacy
• Physical Security Officer
• Physician Recruitment and Services
• Policy Administration
• Privacy Officer
• Quality Assurance
• Radiology
• Respiratory
• Senior Management / Executive Officers
• Skilled Care / Rehabilitation
• Support Services
• System Users
• Systems Administration
• Trading Partners
• Underwriting / Statistics
• Volunteer Services

The Functional Areas listed are just the defaults, and can be modified according to how your medical establishment is setup. You may need to add new Functional Areas such as Oncology or Pediatrics and HIPAA-Watch allows you to do that.
Once a Respondent has been designated for each Functional Area, appropriate audit questions are assigned to each Respondent. The survey of questions is extensive. Sample questions include the following:

- Does your organization retain HIPAA security documentation for six years from the date of creation?
- The network automatically scans PCs and workstations for viruses before allowing users to access the network?
- Network servers, peripheral devices, and communications equipment are kept in secured areas?
- There is an up to date list of all vendors and support personnel who are authorized to enter your building or facility?
- Access to system log data is restricted to approved personnel?

When you are setting up the survey questions, it is possible to reference the actual HIPAA control standards with the individual sections cited by their Code of Federal Regulations (CFR) number, depicted in Figure 3.
Question sets can be prepared for the first time, or imported from previously composed question set libraries. Upon final configuration of the question sets, Phase III begins.

A highlight of HIPAA-Watch is the flexibility of the survey process. Respondents can be surveyed automatically over a server or over the web, questionnaires can be e-mailed directly, or question diskettes can be created and distributed throughout the organization. Answers are directly imported back into the appropriate case and compiled with audit trails.

Phase III launches the risk analysis engine and performs the evaluation. Clearly preparing for the evaluation is a lot more time consuming than running the evaluation engine. Before you actually run the evaluation however, HIPAA-Watch allows you to review the links created between Asset Categories with Loss Categories. If you need to change the default recommendations for the links between Asset Categories and Loss Categories, it is simple to make the change. You simply uncheck the assets that are not prone to the type of loss indicated. For example, Supplies and Consumables are likely not prone to Data Disclosure and therefore should not be linked. Figure 4. illustrates how Assets are linked to Losses.
In Phase III, you decide which calculations you want to compute based on the relationships of the threats, assets, vulnerabilities, and seriousness of potential incidents.

Phase IV generates a final report that has a variety of options that can be included. The options include:

- An Executive Summary
- Recommendations for Resolving Vulnerabilities
- A Full Asset Report
- A Summary by Asset Report
- A Full Threat Report
- A Summary by Threat Report
- A Full Vulnerability Report
- A Vulnerability Distribution Report
- A Full Safeguard Report
- A Cost Benefit Report
- A Safeguard Threat Report
- An Audit Trail Question Report
- An Audit Trail Respondent Report

The reports generate color pie charts and bar charts and can be saved in either Rich Text Format or Microsoft Word Format. While the reports are verbose in their recommendations, most organizations will want to apply some edits to customize them further.

**Suggestions for Product Improvement**

Relevant Technologies would like to see the aesthetics of the user interface improved in HIPAA-Watch for Security™. The engineering of the tool is so sophisticated, that this product deserves a user interface with cutting edge aesthetics and a vanguard look. While the existing graphic design and reporting engine is adequate, it could evolve into a market sensation if the developers enlisted the help of a top-notch
design artist. Relevant Technologies believes that software is art, and when a product excels, we expect the look and feel of it to excel also. The look and feel of HIPAA-Watch for Security™ is basic and for that reason, using it may not elicit as many oos and ahs as it might otherwise given its capabilities.

Relevant Technologies would prefer to see the survey questions worded in the form of a true interrogative sentence instead of a statement with a question mark at the end. For example, instead of "Access to system log data is restricted to approved personnel?" we would prefer the question to be worded, "Is access to system log data restricted to approved personnel?" However, it's fair to say that the survey questions that exist are certainly on topic and apropos to a HIPAA audit.

Since LAFE values vary according to geographic location, Relevant Technologies would like to see this feature automated so that when you put in your organization's Zip Code, the LAFE values are automatically adjusted. For example, if your organization is in Omaha, Nebraska, you would have a much higher likelihood of tornados that if your organization is in Portland, Maine. Today HIPAA Watch for Security™ allows you to manually adjust these values, however, this presumes that you know what the adjustment should be and it may take you some time to look it up and find out.

**Recommendations for Users**

HIPAA-Watch for Security™ works as advertised and has all the appropriate features that experts in risk analysis expect to see. It's ability to make appropriate calculations from which quantitative risk-based decisions can be made is first-rate. The automated reports that it generates will be useful for Chief Financial Officers, Chief Information Officers, and Chief Security and Privacy Officers. Since HIPAA-Watch for Security™ has the ability to accommodate multiple respondents that can login to the system from different locations, it can be particularly useful for large, disparate organizations. By using HIPAA-Watch for Security™ it is possible to understand which safeguards will give you the greatest return on investment, ranking them from highest to lowest. If you are ready to tackle a HIPAA compliance risk analysis, and don't know where to start, using HIPAA-Watch for Security™ will likely speed up your ability to comply with the CFRs.

Aside from helping your organization comply with the Final Security Rule, HIPAA-Watch can help your organization make better business decisions by making recommendations on how cost effective it is to apply particular safeguards. To take advantage of the sophisticated business decision recommendations, users of HIPAA-Watch may want to educate themselves on basic quantitative risk analysis equations including how to calculate Annualized Loss Expectancy (ALE), Single Loss Expectancy (SLE), Annualized Rate of Occurrence (ARO), and Exposure Factor (EF). The information HIPAA-Watch generates can also be used to populate a Disaster Recovery planning exercise.

An auxiliary addition to HIPAA-Watch is a Bonus CD that includes a Data Collection Kit, that has forms, PowerPoint presentations and various short cuts and tips that will make the analyst's job easier. A complete risk analysis project plan is included both in Microsoft Project and in Excel formats for reference purposes.

Consultancies that specialize in assisting healthcare organizations on the road to HIPAA compliance may want to consider using HIPAA-Watch for Security™ as a tool for standardizing their service offering. Since the audit questions can be refined and added to, it is possible to build up comprehensive question libraries that can be used with different types of covered entities. The different types of covered entities that can take advantage of HIPAA-Watch for Security™ include:
Health Care Providers include hospitals, doctors, clinics, pharmacists, and mental health care specialists. Health Care Plans include insurance companies, Health Maintenance Organizations (HMOs), Medicare Plans, Medicaid Plans, Veteran's Health Care Programs, and Indian Health Service Programs. Health Care Clearinghouses include organizations that process or facilitate billing or transmittal of electronic health information data for other covered entities such as community or local health information systems.

Conducting a risk analysis manually is not an intuitive process and use of HIPAA Watch for Security™ will be a definite time saver for any organization that wants to conduct a true risk analysis. A two-day training class is available every month at RiskWatch's headquarters in Annapolis.

A feature that Relevant Technologies found to be particularly notable was the ability to actually see the HIPAA Final Security Rule, which is expressed as a Control Standard. This feature enables organizations to actually understand why they need to pay attention to a particular security policy and whether or not it is considered a Required or Addressable CFR. While Required CFRs are mandatory, Addressable CFRs are optional.

Relevant Technologies spent a considerable amount of time researching possible market competitors and was not able to find any other HIPAA security compliance products that appeared competitive with HIPAA-Watch for Security™. However, since the market for HIPAA compliance products is still young, Relevant Technologies expects new competing products to emerge within the coming year.

U.S. federal agencies will like that the safeguards list includes the deliverables that are typically required to pass a FISMA based security certification and accreditation audit. Federal agencies that already have a Certification and Accreditation (C&A) Package can apply these C&A reports to their HIPAA risk analysis and reuse much of the pre-existing information.

References


Pabrai, Uday, Getting Started with HIPAA, Premier Press, © 2003

SANS Institute, HIPAA Security Implementation, SANS Press, Version 1.0 © January 2004

Taylor, Laura, Risk Analysis Tools & How They Work, Relevant Technologies, Inc.  
http://www.riskwatch.com/Press/RiskAnalysis_Tool_EvalB.htm  
© May 5, 2002

Taylor, Laura, Security Scanning is not Risk Analysis, Jupiter Media  
http://www.intranetjournal.com/articles/200207/pse_07_14_02a.html  
© July 14, 2002

Auerbach Publications, © 2004

© Copyright 2004, Relevant Technologies, Inc. All rights reserved.