

TRACER™



Risk Analysis Solutions



HIPAA & HITECH Require Risk Analysis

A key requirement of the HIPAA and HITECH regulations is that covered entities and business associates *must conduct a comprehensive and thorough assessment of the potentials risks and vulnerabilities to the confidentiality, integrity, and availability (CIA) of all electronic Protected Health Information (EPHI)*. These HIPAA and HITECH mandates require that organizations must complete a comprehensive and thorough vulnerability assessment on a regular schedule.

OCR Guidance on Risk Analysis

The Office of Civil Rights published guidance on risk analysis on July 14th, 2010. That guidance clearly states that, “Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule. Therefore, a risk analysis is foundational...”. Further, OCR tells us that, “All EPHI created, received, maintained or transmitted by an organization is subject to the Security Rule. The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to

implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of e-PHI. Risk analysis is the first step in that process.” ecfirst’s TRACER program satisfies this foundational requirement.

Meaningful Use Requirements Include Risk Analysis

Demonstrating Meaningful Use of an Electronic Health Record (EHR) requirement number 15 tells organizations that they must, “Implement systems to protect the privacy and security of patient data.” Organizations seeking to demonstrate Meaningful Use must, “Conduct or review a security risk analysis and implement security updates as necessary, and correct identified security deficiencies.” ecfirst’s TRACER program satisfies this Meaningful Use requirement.

TRACER – An ecfirst Risk Analysis Service

ecfirst developed the TRACER program to assist Covered Entities, Business Associates, and vendors of Electronic Health Records (EHRs) and Personal Health Records (PHRs) in meeting the requirements of the HIPAA Privacy and Security Rule, The HITECH Act, and all subsequent guidance documentation and settlement agreements.

As a part of the TRACER program, ecfirst will list every requirement of the HIPAA Security Rule including every Safeguard, Standard, and Implementation Specification in a risk analysis format that identifies an organization’s state of compliance with the requirement, recommended remediation activity, and associated risk priority. All remediation activities will be listed according to recommended implementation time bands in the TRACER Corrective Action Plan (CAP) table. The TRACER report is an actionable, documented risk analysis that provides both in depth and executive summary level findings appropriate to all audiences from administrators to the Board of Directors.

TRACER – An ecfirst Privacy Gap Assessment Service

TRACER helps an organization to understand, improve, or verify their compliance with the HIPAA Privacy Rule. TRACER provides both summary and detailed compliance information as well as all necessary remediation activities pertinent to the organization’s business model. TRACER will enable an organization to quickly determine the state of compliance, needed remediation, and will list actionable steps to achieve compliance.

TRACER – An ecfirst Vulnerability Assessment Service

The Office of Civil Rights (OCR) is seeking to ensure that organizations have identified all of the risks and vulnerabilities to the EPHI that they collect, store, process, or transmit. TRACER is an ecfirst program that includes a technical vulnerability assessment to address HIPAA and HITECH mandates with the objective of establishing and prioritizing compliance and security gaps.

The TRACER ecfirst Technical Vulnerability Assessment Service supports several distinct components, including:

- External Assessment
- Internal Assessment
- Firewall Assessment
- Wireless Assessment
- Social Engineering

When is the last time your organization conducted a risk analysis activity that included a technical vulnerability assessment?

TRACER addresses vulnerability assessment in the following areas:

- Passwords transmitted in the clear
- "Open" holes and exploitable attack vectors
- Active Directory audit
- SNMP audit
- Oracle and SQL database audit
- Router and Switch audit
- Firewall rules and configuration audit
- Network vulnerability scan

The TRACER report includes a complete remediation plan to address gaps identified. The report includes a dashboard, executive summary, and suggestions for remediation.

External Network Vulnerability Assessment

ecfirst will identify, analyze, and document vulnerabilities within an organization's Internet-facing infrastructure and attached systems. ecfirst follows a pragmatic approach when conducting a vulnerability assessment of external systems.

Internal Network Vulnerability Assessment

ecfirst's internal network vulnerability assessment will verify that the security controls implemented on an organization's hosts provide an adequate level of protection against network attacks. The ecfirst security team will scan and validate the security of the network and perform a comprehensive assessment against selected hosts. ecfirst can include many valuable components in its reporting including:

- Active Directory assessment
- Open File Shares scan and report
- SNMP scan
- Promiscuous NICs scan and report
- Database Security Analysis including MS SQL or Oracle

Firewall Assessment

ecfirst will review the organization's Internet-facing firewall to identify the current security posture in three critical areas:

- Rulebase configuration
- Current IOS (or other operating system) and patch revision release level
- Vulnerability assessment of configuration file

Rulebase configuration is critical to the integrity and operating security of a firewall. The rulebase should be tied to business requirements. Every rule that is configured on a firewall is essentially a permissible security hole into the company's network infrastructure. Each of these rules should have a well defined business need for existing. However, many corporations open rules for testing and never close them when the test has completed. Additionally, many rules are opened up because of then-current business needs, but never closed or repaired once that need, or the corresponding business contract, has ended. This results in legacy access and a vulnerability providing a pathway into the internal network.

Wireless Assessment

Wireless networks are particularly vulnerable to attacks because it is extremely difficult to prevent physical access to them. Wireless networks are subject to both passive and active attacks. A passive attack is one in which an attacker just captures signals flowing from authorized devices, such as a corporate laptop to an authorized Access Point (AP). An active attack is one in which an attacker send signals to the authorized AP in order to solicit specific responses and intrude upon the corporate network, typically, in a very short timeframe.

During the wireless assessment, ecfirst will address the following areas:

- Discover the Wireless Access Points and wireless systems.
- Investigate rogue devices installed without IT department consent.
- Assess WiFi RF coverage trying to sniff from adjacent buildings and public locations.
- Determine the existing WiFi security infrastructure.
- Attempt to compromise the wireless security.
- Determine encryption type and compromise the security.

Social Engineering Assessment

Companies with excellent security programs often spend large amounts of money on capital purchases to implement technical security controls. However, employees or contractors of the entity often prove to be the weak link in the security chain. Employee and contractor education is a key component to any information security program. Authorized members of the workforce have both authenticated access to information systems as well as physical access to facilities and secured areas. Responsible enterprises assess Human Resources security gaps as well as technical vulnerabilities.

During the social engineering assessment, ecfirst will attempt to gain unauthorized or inappropriate access to facilities, secured areas, documents, credentials, or confidential data. ecfirst security personnel will attempt to bypass security controls that are in-place in order to gain access to various assets. ecfirst will attempt to bypass electronic, personnel, and procedural controls during this assessment.

ecfirst will document and present a very detailed record of successes, failures, controls bypassed, access achieved and information obtained during the assessment. ecfirst will

also deliver recommendations for personnel security enhancement needs and security controls requiring improvement or replacement as a part of the final report.

TRACER – An ecfirst HITECH Data Breach Service

Under the HITECH Data Breach Rule, organizations are required to take steps to prevent, identify, report, and remediate data breaches of unsecured information. The ecfirst TRACER solution will document the ability of the organization to detect a breach, review the incident management policy and procedures, and make recommendations. In addition, organizations will receive a HITECH Data Breach policy and several Data Breach procedures to ensure compliance, should a breach happen.

ecfirst Differentiators

ecfirst combines state of the art tools, the highest credentialed staff, and reporting that maximizes value, efficiency, and information for our clients to deliver the industry's best technical vulnerability assessments.

Critical ecfirst differentiators include:

- Highly credential professional team
- Deep experience in the healthcare industry
- Compliance based vulnerability assessments
- Executive dashboards that are tailored for senior management to highlight critical findings

ecfirst utilizes tools that are constantly updated to ensure that clients are aware of all of the vulnerabilities on their networks and systems. These include technical vulnerabilities all the way up to “zero day attacks”, DNS vulnerabilities, Active Directory and database vulnerabilities, as well as information available in the public domain about our clients.

ecfirst deploys only highly credentialed and very experienced experts to client sites to perform vulnerability assessments. ecfirst engineers possess certifications such as CISSP, CISA, and CEH and have performed numerous assessments at clients spanning multiple industries. Our engineers understand the sensitivity and criticality of your systems.

Our clients benefit from the most useful reports in the industry. ecfirst provides our clients with descriptive reports that contain real world recommendations. Sections are included for both executive level audiences and the most technical engineer. Executive summaries draw out the most critical and pressing issues for quick comprehension and dissemination.

Contact Us

Please contact John Schelewitz at John.Schelewitz@ecfirst.com or at +1.480.663.3225 to learn more about the ecfirst BizShield™ TRACER Technical Vulnerability Assessment solutions to address critical compliance mandates. We would like to understand the regulations that impact your organization as well as your security

challenges to determine how ecfirst can augment your efforts to achieve compliance with federal and state mandates..

Talk to us – you will find us to be a partner you can trust.

About ecfirst

ecfirst delivers world-class information security and regulatory compliance solutions. With over 1,600+ clients, ecfirst was recognized as an Inc. 500 business – America's Top 500 Fastest Growing Privately Held Business in 2004 – our first year of eligibility. ecfirst assists organizations with their compliance initiatives for a secure information infrastructure that is compliant with regulations such as HITECH, HIPAA, ISO 27000, or federal and state legislations (such as California or Massachusetts).

ecfirst serves a Who's Who client list that includes technology firms, numerous hospitals, state and county governments, and hundreds of businesses across the United States and abroad. A partial list of clients includes Microsoft, Symantec, HP, McKesson, EMC, IBM, Principal Financial, U.S. Army, U.S. Dept. of Homeland Security, U.S. Dept. of Veterans Affairs and many others.

Talk to ecfirst and you will find an organization that is passionate about the services we deliver and exceptionally devoted to its clients.

We deliver value with intensity and are paranoid about our performance for your organization.

For more information, please visit <http://www.ecfirst.com/>.