



Technical Vulnerability Assessment 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.

TRACER – An ecfirst Vulnerability Assessment Service

TRACER is an ecfirst program targeted in the area of technical vulnerability assessment to address HIPAA and HITECH mandates with the objective of establishing and prioritizing compliance and security gaps.

TRACER - an ecfirst Technical Vulnerability Assessment Service – supports several distinct components, including:

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

Regulations such as the HIPAA Security Rule and HITECH require organizations (covered entities and business associates) to conduct a thorough and comprehensive risk analysis activity on a regular schedule. This is a federal mandate.

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

What Does TRACER Do?

TRACER addresses vulnerability assessment in the following areas:

- Malicious or suspicious network traffic
- "Open" holes related to attack vectors
- Full Active Directory audit
- SNMP audit
- Oracle database audit
- SQL database audit
- Insecure driver vulnerability scan
- Router audit
- Firewall rules audit
- Switch audit
- Full network vulnerability scan

The TRACER report includes a complete remediation plan to address gaps identified. The TRACER service offering may be packaged to deliver to you monthly and quarterly reports can be customized for executive management.

External Network Penetration Assessment

ecfirst will identify and deeply analyze 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 Penetration 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:

- Open File Shares scan and report

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

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

BizShield™ TRACER Vulnerability Assessment Solutions from ecfirst

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.

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 1,500+ 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

BizShield™ TRACER Vulnerability Assessment Solutions from ecfirst

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/>.