



*Excellence in
IT Security & Investigations*

CASE STUDY 4: MEDICAL RECORDS, CLIENT LISTS, PRICING SCHEDULES

INDUSTRY: HEALTHCARE

POTENTIAL LOSS: \$800 MILLION +

CHALLENGE: HIPAA VIOLATIONS, IT SECURITY ASSESSMENT

TIME TO RESOLVE: 14 DAYS

Background: Following the reports of hackers stealing customer data from major companies such as T.J. Maxx, the C.E.O. of a large healthcare organization, with millions of patient records, called us in to perform a due diligence penetration test and to assess the IT security posture of the corporation.

Challenge: Cyber Diligence was asked to conduct a limited penetration test and Mid-level IT Security Assessment to determine the cyber security posture at two large divisions of the organization. The C.E.O of the company explained that loss of his customer lists, pricing and supplier schedules to a competitor would cost his company hundreds of millions annually in lost revenue. With more than 8 million patient records, the loss, theft or breach of security of those records had potential fines in excess of \$800 Million.

Response: Cyber Diligence performed a “black box” penetration test of both the company’s web based email system and their wireless system. This included use of a laptop in the parking lot outside the corporate building housing the company’s call center, billing offices and IT department to launch a Wi-Fi attack similar to that which occurred in the T.J. Maxx incident. Afterwards a mid-level on-site IT security assessment was then undertaken including the interviews of key business process owners, randomly selected employees, and IT personnel. A review of IT security logs and the system’s network architecture was also conducted.

Results: Within 15 minutes, members of the Cyber Diligence team were able to successfully penetrate the wireless network from the company’s parking lot, then access a large number of servers including the patient database, open accounts and place a document file in the root directory of the corporate system which stated “This server is compromised as a result of an authorized penetration test conducted by Cyber Diligence, please call (000) 000-000 to report this event”. No security logs or intrusion mechanisms employed by the company detected this event. A check of the network revealed that manufacturer recommended patches and security upgrades on 30 randomly selected servers were not implemented by the IT Department. One-third of all workstations had active USB hubs; this exposed the company to “insider theft” wherein an employee could download sensitive information to a portable storage device. Further examination also revealed that the vendor who supplied their customer order processing software dropped its support because an in-house software developer had re-programmed and made customized adjustments to that software numerous times. There was no documentation of these changes and all IT support was reliant on this one individual, and the loss of this employee would be devastating to the company. Employee access codes and passwords were not changed on a regular basis, nor were they removed when employees left the company. During routine innocent conversations, two of three employees quickly revealed their access codes and passwords to the Cyber Diligence staff.

A check of business records indicated that the firm had just one month before passed a SOX compliance audit of their IT functions by a major auditing organization.

Important Notes: In a September 2, 2009 article “Is Your Health Privacy at Risk?” published in Network World magazine, Carolyn Duffy Marsan reports that hospitals, pharmacies and health insurance companies are among the hardest hit when it comes to hacker attacks, stolen laptops, spying employees and other information security mishaps.

ABOUT CYBER DILIGENCE, INC.

Founded by Mr. Yalkin Demirkaya (NYPD Retired) Cyber Diligence is comprised of highly trained investigators who are world-recognized experts in information security (INFOSEC), Incident Response, Investigations and security management. Cyber Diligence Investigators are experienced criminal investigators who are also skilled at deploying sophisticated state-of-the-art tools to combat Information Technology crimes and to counter intrusions that compromise valuable corporate assets.

Cyber Diligence specializes in conducting highly sensitive covert internal investigations. Our expertise includes:

- Insider abuse detection
- Investigations into actual or suspected industrial espionage
- Electronic Discovery Services
- Litigation Support/Expert Testimony
- Incident Response
- Computer Forensics
- Network Forensics
- IT Security Assessments
- Intellectual Property Protection
- Malicious activities and other forms of misconduct or corporate compliance violations.
- Counter-Surveillance Services (Technical Surveillance Counter Measures)

Cyber Diligence is a licensed Private Investigations firm, whose investigative team members are former law enforcement investigators and commanders. They possess over 140 years of investigative experience and have successfully investigated many high level industrial espionage cases in the United States and abroad.

WHY CYBER DILIGENCE?

1. We have the knowledge, skills and experience.
2. We have a state-of-the-art lab equipped with the latest computer and network forensic tools to tackle any cyber security incident. We attack the problem with the right tools.
3. We have a unique IT assessment methodology to assess an organization's IT security posture to protect against internal & external threats.
4. Qualified people with years of computer crime investigative experience ask qualified questions – we trust the answers, but we always verify.
5. We take a realistic approach to your business, understanding your culture to secure your business with common sense solutions.

Contact Us: info@CyberDiligence.com

WWW.CyberDiligence.com Phone: 516-342-9378 | Fax: 516-605-0862 | 575 Underhill Blvd. Suite 209 Syosset, NY 11791