Combating Threats to Protected Health Information

- By V Balasubramanian

ManageEngine has co-sponsored the “Protected Health Information (PHI) Project,” an initiative launched by the American National Standards Institute (ANSI) to evaluate the financial impact of unauthorized access to Protected Health Information (PHI).

This paper draws information from the report "The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security".

Unauthorized access and use of protected health information is the most profitable crime in the USA

Are you fully prepared to combat?

At over $60 billion per year, Medicare fraud has become one of the most profitable crimes in America, say analysts. In South Florida, health information fraud has replaced cocaine as the major criminal enterprise. As health care providers have fully turned digital with Electronic Health Records that contain protected health information, health information data breaches are also increasing in number, frequency and magnitude across the globe.

It might be baffling to some – what would one gain from stealing protected health information. Fraud resulting from medical identity theft primarily takes two forms:

1. physician identification numbers that are stolen and used to bill for services, and
2. patient identification information stolen (or lent to friends and relatives) and used to obtain services or to bill for services

Illegally accessing health information details of prominent celebrities also often proves highly profitable for cyber-criminals.

Individuals tend to disclose the most intimate details about themselves to their doctors only with the trust that their health information will remain private and secure, whether it resides in a file at their doctor's office, on a hospital chart, or in a claims form at their insurance provider.

Unfortunately, growing incidents of fraudulent access and use of protected health information (PHI) suggest that not all organizations entrusted with PHI protection are upholding their responsibility. PHI breaches cause significant harm, both to the individuals whose information was breached and to the organizations responsible for protecting it. Consequences of PHI breach for organizations are still more serious - loss of trust, financial loss, operational issues, legal hurdles and in extreme cases, even of loss of business.

PHI – Stakeholders and their Responsibilities

Protected health care information is being handled by a large number of stakeholders – physicians, therapists, clinics, hospitals, laboratories, pharmacists, insurers, insurance companies, law firms, telemedicine firms and other agencies.

These stakeholders are responsible for the confidentiality, integrity, and availability of all PHI they create, receive, maintain, transmit, or store. This responsibility includes implementing appropriate safeguards against any reasonably anticipated threats or hazards to the security or integrity of that information. They must ensure:

- Confidentiality: data or information is not made available or disclosed to unauthorized persons or processes
- Integrity: data or information has not been altered or destroyed in an unauthorized manner
- Availability: data or information is accessible and useable upon demand by an authorized person

PHI - Threats & Vulnerabilities

Threats for protected health information emanate both from external attacks and internal sources.

External Attacks – Health care enterprises come into contact with a variety of people in a variety of ways. Sensitive information and IT resources need to be exposed or shared with partners, agencies and even customers. All these make the enterprises vulnerable to data breaches and cyber-attacks from amateur and expert hackers.

Internal Threats - Threat to information security does not always develop from outside. It could well be generating right inside the organization. Disgruntled staff, greedy techies, tech-savvy contractors and sacked employees could act with malicious intent and misuse privileged access. Even untrained staff could unintentionally unleash a disaster. The business and reputation of some of the world's mightiest organizations have been shattered in the past by a handful of malicious insiders.

Researchers point out that more than half of data breaches involve the participation of an insider, but only 10% are unintentional – whereas 90% are deliberate and malicious and usually involve misuse of privileges.

How to combat?

Preventing or detecting a breach requires that effective policies, procedures, and technologies are in place. Without proper technology in place, policies and procedures would remain ineffective and cannot be enforced. The CISOs, CIOs, IT security, privacy, and compliance personnel of health care organizations, who are tasked with the responsibility of protecting PHI should keep in mind the fact that the benefits of investing in technologies to prevent PHI breach, far more outweigh the potential cost involved in setting them up.

A report on "**The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security**", created through the "PHI Project" – a collaboration of the American National Standards Institute (ANSI), via its Identity Theft Prevention and Identity Management Standards Panel (IDSP), in partnership with The Santa Fe Group/Shared Assessments Program Healthcare Working Group, and the Internet Security Alliance (ISA) – that involved a cross-section of more than 100 health care industry leaders from over seventy organizations, underscores the importance of the information security technical safeguards as required by HIPAA Final Security Rule 164.312, which includes:

Access Control: Protect ePHI from unauthorized disclosure

- Allow system access only to authorized persons or applications
- For a web environment, implement a web access management solution
- Consider role-based access control
- Assign unique user identification
- Ensure the use, monitoring, and audit recording of emergency credentials
- Establish automatic logoff and re-authentication after a period of inactivity
- Limit access to encrypted applications to those who can decrypt the data

Integrity of Audit Controls: Protect information from alteration or destruction

- Implement mechanism to authenticate ePHI
- Implement methods to corroborate that information has not been altered or destroyed

Transmission Security: Protect ePHI that is being transmitted over a network

- Consider encryption for best protection and safe harbor
- Ensure strong encryption up to 2048 bits (asymmetric) and 128 bits (symmetric)
- Verify data integrity with digital signatures or SSL certificates

The recommendations of the PHI project to secure PHI lay stress on the following technological aspects, in addition to the procedural and policy enforcement:

- Risk management (risk identification, threat analysis, etc.)
- Asset management (physical and information)
- Identity management (user IDs, passwords, etc.)
- Vulnerability management (secure configuration, patches, etc.)
- Operations management (logs, laptops, desktops, change management, network, mobile devices, removable media, etc.)
- Information protection (encryption, key management, etc.)
- Threat management (intrusion detection, incident response, etc.)
- Security control testing (penetrations testing, audits, etc.)

Multi-pronged Strategy – Need of the Hour

Combating sophisticated cyber threats involving protected health information mandates a multi-pronged strategy incorporating a complex set activities including deploying security devices, enforcing security policies, controlling access to resources, monitoring events, analyzing logs, detecting vulnerabilities, managing patches, tracking changes, ensuring compliance, monitoring traffic and other activities.

ManageEngine has a range of affordable **Enterprise Security Management Software Solutions** that help you **build a secure fortress** enabling you to protect PHI, stay secure, ensure business continuity and enhance productivity.

A Strong Perimeter

Identify vulnerabilities & secure your boundary

The first step in building a fortress is to secure your boundary, understand your vulnerabilities and initiate action for protection. For a strong perimeter in enterprises, you must:

- scan your network, create inventory of network assets
- identify network vulnerabilities & remediate them swiftly
- detect missing patches, hot-fixes & security updates on Windows and Linux and deploy them quickly
- manage changes to Windows files, folders and registry
- stay informed with audit reports on open ports, hardware and software

Try Security Manager Plus! www.securitymanagerplus.com

A Secret Chamber

Protect the keys to your kingdom

After building the fortress, the keys to your kingdom need to be protected. A strong perimeter just protects you from external attacks. But, to guard yourself from malicious insiders, you need a secure, centralized 'secret chamber' for safe upkeep of the keys and control over privileged access to a select few. In enterprises, you need to:

- securely store, manage and control access to shared sensitive information such as passwords, documents and digital identities
- eliminate password fatigue and security lapses
- improve IT productivity many times by automating frequent password changes required in critical systems
- establish preventive & detective security controls through approval workflows & real-time alerts on password access
- meet security audits and regulatory compliances such as SOX, HIPAA and PCI

Try Password Manager Pro! www.passwordmanagerpro.com

The Citadel

Establish a centralized authority for network device configurations

In the fortress, the citadel is the seat of the centralized authority and is the strongest component. In enterprises, network devices are the crucial components. Any unauthorized configuration change could wreak havoc on the network. To secure device configurations, you need to

- automate backup of configurations of switches, routers, firewalls & other devices
- track configuration changes in real-time & generate notifications
- prevent unauthorized configuration changes
- control access to configurations & enforce role-based restrictions for configuration upload
- check configurations for compliance to policies & standards
- get complete record of 'who', 'what' and 'when' of device configuration changes
- automate the entire life-cycle of device configuration tasks

Try DeviceExpert! www.deviceexpert.com

The Operational Command Center

Constitute centralized control for servers & desktops

In the fortress, day-to-day operations are controlled from the command center. Likewise, in enterprises, servers and desktops constitute the nerve centre of routine operations. Securely managing them from a centralized location is a crucial task, which requires you to:

- automate the desktop management routines of enterprises to standardize and secure their Windows network
- protect desktops from wide range of threats
- quickly troubleshoot of day-to-day issues
- generate comprehensive reports to audit IT assets

Try Desktop Central www.desktopcentral.com

The Watch Towers

Monitor, analyze log data and alert on internal, external security threats

Watch Towers in the fortress help in observing the happenings around and protect from potential threats. In enterprises, keeping a watchful eye over the eventlog, application log and trails from perimeter security devices is essential to safeguard the organization from evolving internal and external threats and optimize performance. This mandates:

- automatically collecting, analyzing, reporting, alerting and archiving event log from distributed Windows hosts, Syslog from Unix hosts and devices & Application log from servers and databases
- monitoring, analyzing and reporting on logs from firewalls and other perimeter security devices
- troubleshooting network problems and optimize bandwidth usage & performance
- complete visibility on internal & external security threats
- meeting regulatory audit and compliance requirements

Try Firewall Analyzer & Eventlog Analyzer www.firewallanalyzer.com , www.eventloganalyzer.com

Related Products

ADManager Plus

A comprehensive and web-based Active Directory management and reporting software. Using ADManager Plus, automate time-consuming and painstaking administrative tasks such as user creation/modification/deletion; reduce administrative burden through helpdesk delegation; and generate compliance-specific reports.

www.admanagerplus.com

ADAudit Plus

An enterprise-wide Active Directory change auditing and reporting software so you can track each and every change in Active Directory; fulfill compliance requirements set forth by regulatory acts; and boost AD security through timely alerts and critical reports.

www.adauditplus.com