PROFICIO™

How Healthcare Organizations Can Avoid Damaging Security Incidents and Loss of Patient Data

Your organization has just had a security breach and now you have to notify your management. You need to call your boss. This is never an easy call and invariably includes questions like: What data has been compromised?
How bad is it and do we need to report a PHI disclosure?
How and when did you find out about this?
Have we closed the security hole?
I thought we passed an audit or assessment recently.
Why didn't that new security product you just bought stop this?

You may have been fortunate and found the problem quickly, contained it, and can reassure your management that the expo-sure is limited.

Reality is often different. Studies by Proficio, Verizon, and others show that the majority of security incidents are discovered by third parties, and in two thirds of the cases not detected for a month or longer. Once detected over half of the cases took a week or more to contain.

Hackers like to target healthcare organizations

Cyber criminals target patient records, SSNs, and credit card numbers. Foreign actors are searching for intellectual property including proprietary medical research and processes.

Medical identity theft is growing and is a significant problem. According to the 2013 Survey on Medical Identity Theft conducted by Ponemon Institute, medical identity theft affects nearly 2 million people and has increased 20% in the last year.

Healthcare organizations are considered soft targets for the following reasons:

1. Their security departments are often under-staffed relative to other similarly sized organizations in other industries.
2. Hospitals are harder to defend because they have complex systems, multiple locations, diverse departmental applications, and patient and physician web portals.
3. Many hospitals are associated with university campuses and are vulnerable through their connection to university networks that have porous perimeter security.
4. Visiting physicians, consultants, and contractors need access to healthcare networks and accentuate the risk of insider threats, password compromises, and exposures due to misconfiguration of systems or devices.
5. Embedded operating systems in medical devices frequently have known security vulnerabilities that IT staffs are unable to patch.
6. Healthcare organizations increasingly rely on cloud-based services, applications and data storage. Third party cloud-based services focus on protecting their service leaving their clients to deploy virtual intrusion detection software and monitor logs in the cloud.

Increasing cost of data breaches

The consequences of PHI disclosures, credit card theft, and other types of confidential data loss are significant and include:

Increased penalties for HIPAA violations were included in the 2013 Omnibus Final Rule. Fines now begin at $100 per violation and go up to a $1.5 million annual maximum liability for violations of an identical rule.

Litigation costs and settlements associated with security breaches are very large and growing, and escalate substantially if discovery determines the organization has not followed the current HIPAA security regulations for areas like logging security events and actively monitoring security logs.

The loss of reputation and brand value from bad publicity have a negative impact on the stock price of public companies, and reduces the ability of not-for-profit organizations to raise funds. Brand reputation is also directly related to recruiting, research grants, and patient confidence in medical outcomes.

Remediation costs include third party forensic consultants to investigate the root cause of a security incident, services to communicate with individuals affected by the breach, and PR consultants who specialize in mitigating the effect of harmful events.

Lengthy delays are inevitable when dealing with the aftermath of a security breach. Remediation can create hundreds of man-hours of work for IT organizations and distract staff from other priorities and critical projects.

Real world security incidents and how they can be prevented

Unfortunately, the number and severity of security incidents affecting healthcare organizations is growing. This trend is understated as it does not include attacks that are never discovered by the targeted organizations. There is no good data on the impact of Advanced Persistent Threats (APTs), next-generation malware and various types of stealthy exploits that are designed to exfiltrate data without being detected.
Proficio has worked extensively with healthcare providers and their partners that process and store Protected Health Information (PHI). The following are examples of real security incidents and recommendations on how they could be avoided.

An employee has been found leaking confidential patient information

Employees who inappropriately access the medical records of patients, expose their organizations to fines, law suits, and negative publicity. This activity can range from inappropriate curiosity into a celebrity's medical condition to actual theft and sale of protected health information.

Recommended Countermeasures
Patient Privacy Monitoring: Applications like FairWarning and Cerner's P2 Sentinel track end-user access to confidential patient data. We recommend maximizing the value of these systems by using either a managed security service provider (MSSP) or a SIEM system to collect logs from application monitoring systems and correlate anomalous access of medical records with other events like suspicious logins, saving files to USB drives, or unusual email activity. A single event, such as a nurse inappropriately accessing a VIP's medical records, might go unnoticed. By adding the nurse to a watch list, a high priority alert can be generated if this behavior reoccurs. Correlated alerts should be monitored 24x7 by a Security Operations Center (SOC) staffed by certified analysts.

Privileged Account Management: Disgruntled employees with administrative account access can configure their privileges to snoop medical records. Administrative accounts should be monitored and protected by complex passwords. Passwords should be changed or expire on a regular schedule and when administrators leave the organization. SIEM systems should monitor applications for unusual activity, such as after hours access using administrative privileges.

Medical devices with unpatched security vulnerabilities are exposed to attacks compromising patient care

Networked medical devices can create a challenge for hospital security teams because they do not control the process of upgrading the underlying operating system embedded into these devices. Many medical devices using older versions of Windows and Linux have known security vulnerabilities and are at risk of malware contamination and security exploits.

Recommended Countermeasures
Regular Vulnerability Scanning: Regularly scan medical devices for vulnerabilities and malware.

Protect the Perimeter from Malware: Intrusion protection systems and next-generation firewalls, such as TippingPoint and Palo Alto Networks, can identify malware and block it or sandbox it. Reputation services add to the reliability of perimeter security systems by identifying incoming traffic from known sources of malware or spam.

Asset Modeling and Event Correlation: Use an MSSP or SIEM to feed vulnerability scan data into customized correlation rules and use cases that prioritize related events for medical devices with known vulnerabilities. Alert security teams of suspicious events.

We learn that hackers have stolen our confidential information

In addition to patient records, healthcare organizations are responsible for credit card data, intellectual property, and financial data. Hackers are always on the lookout for vulnerabilities in servers, databases and web applications.

Recommended Countermeasures

Asset Modeling and Event Logging: Use an MSSP or SIEM to classify assets with critical data like patient records or credit card numbers. Monitor events such as failed logins to critical assets and apply higher priority to the associated alerts to trigger a review by a Security Analyst.

Identify Threats: Create SIEM correlation rules and use cases that identify attacks from foreign countries or multi-phased attacks like APTs.

Vulnerability Management: Conduct regular vulnerability scans to ensure devices and servers have no unpatched vulnerabilities and are using secure configurations – default passwords and configurations are easy exploits for hackers.

Scan Web Applications: Vulnerabilities in web applications can lead to SQL injections, cross-site scripting, and other code based attacks. Despite the fact that such vulnerabilities are well documented, they account for a significant number of data breaches.

We have been notified that some of our printers have vulnerabilities that can be used to steal PHI

The discovery of new security vulnerabilities in printers is increasing as printers become more sophisticated and have more resources. Hackers know that IT teams do not always prioritize securing networked printers and consider them an attractive target. The impact of confidential information being stolen or disclosed is very real and IT security teams need to take a proactive role to minimize this risk.

Examples of security exploits against networked printers and scanners include:

- Denial of Service (DoS) attacks using malformed SNMP packets to crash printers
- Remote installation of unauthorized printer firmware enabling printed documents to be sent to a hacker
- Printers with hidden URLs hardcoded in the firmware that can be accessed without authentication

Printer vulnerabilities can also be used as a jumping-off point to attack other network resources or in some cases to steal data stored in memory.

Recommended Countermeasures

Use the Printer's Built-in Security Functions: Printers come with a range of security settings. Start by changing the default password and take advantage of any built-in firewall features on the printer, like whitelisting and user authentication. Leading manufacturers regularly patch their printers for security vulnerabilities. Update printer firmware regularly or by default to close known security vulnerabilities.

Protect Your Printers: Ideally, printers should not use public IP addresses and should be behind your firewall to prevent access from untrusted networks.

Vulnerability Scanning: Scan printers to ensure firmware updates occur by default and that SNMP and FTP services are disabled on printers. We recommend you test printers before scanning large numbers as some printers don't handle being scanned very well.

We have been notified that our network is acting as a botnet and some of our public IPs have been blacklisted

Email spammers and hackers use malware tools to penetrate one or several computers and then launch attacks against other networks. For example, infected computers could be used to disrupt other organizations as part of a Distributed Denial of Service (DDoS) attack, or be turned into spambots. Reputation services identify the source IP addresses from such attacks and trigger ISPs, firewalls, IPS, and email security systems to block incoming traffic from these sources.

Traffic activated by malware reduces bandwidth available for legitimate applications and IT teams must undertake time consuming efforts to remove the malware and clear their organizations' reputation.

Recommended Countermeasures

Block Malware at the Perimeter: IPS systems and next-generation firewalls, such as TippingPoint and Palo Alto Networks, can identify malware and block it or sandbox it. Reputation services add to the reliability of perimeter security systems by identifying incoming traffic from known sources of malware or spam.

Use Updated Anti-Virus (AV) Software: All computers, servers, and endpoints should have updated AV software. We also recommend a belt and suspenders approach by scanning for malware at the gateway with advanced malware detections systems. We frequently find malware when customers using commercially reputable AV scanners have found none. The reason is next-generation malware is more difficult to find and hackers test their malware against well known products to ensure they are not detectable.

Prevent Malicious Emails: Email is a primary vector for infecting users with malware. We recommend using a powerful email security system to prevent end-users from downloading malicious attachments like Trojans, or being lured into malware infected websites by phishing attacks.

Monitoring Outbound Traffic: Use an MSSP or a SIEM system to monitor logs and events. By monitoring outbound traffic above normal thresholds, security analysts can investigate endpoints for suspicious types of traffic or destinations. A reputation service will help trigger alerts when outbound traffic is destined for known bad Internet addresses.

Security assessment by a third party consultant reveals our CEO's VoIP phone is being tapped

By injecting malicious code into a VoIP phone it is possible to record private conversations. An attack could be launched by logging into the device over SSH or by plugging into the Aux port of the phone to gain local access.

VoIP phones use the Session Initiation Protocol (SIP). SIP has a number of security vulnerabilities. For example, it is possible for an unauthenticated, remote attacker to launch a Denial of Service (DOS) attack causing the affected device to become unresponsive.

Recommended Countermeasures

Restrict Network Access: Limit access to trusted users and protect the network perimeter with a firewall.

Device Security: Change default passwords and apply other vendor recommended security settings. Restrict or disable web administrative functions. Patch and update to the latest firmware.

Vulnerability Scanning: VoIP phones can be disrupted by automated scanning technology. We recommend a security consultant use manual tools to periodically scan VoIP phones.

Asset Modeling and Monitoring: Use an MSSP or a modern SIEM system to monitor the VoIP phones used by critical users as well as the SIP ports on firewalls. Monitor unauthorized access attempts to administrative interfaces on VoIP phones such as HTTPS or SSH. Correlation rules and use cases should be developed to identify suspicious behavior.

One of our laptops containing unencrypted PHI has been lost or stolen

Stolen or lost laptops with unencrypted patient data comprise a significant percentage of the disclosures governed by HIPAA regulations. Lost or stolen USB drives, CDs, smart phones, and other mobile devices further contribute to the magnitude of this problem.

Recommended Countermeasures

Encrypt Data at Rest: There are a wide range of tools that can be used to encrypt mobile devices and data. Many reported PHI disclosures involve healthcare organizations that already have these tools, but have been slow to implement them. We recommend the use of encryption software that can be centrally managed and supports a broad range of mobiledevices.

Policy-Based Email Encryption: PHI found on laptops is frequently in an email or email attachment. Our recommendation is to apply encryption to any emails that include identifiable patient data. Data Loss Prevention (DLP) systems can identify emails and attachments with medical terms, Patient IDs, SSNs, etc.

We recommend a system that supports selective sender-based remediation.

For example, a hospital administrator may attach a spreadsheet containing information on multiple patients. Options should include temporarily stopping this message and sending a notification back to the sender alerting them of the content within the message, the ability to block the message permanently, or to encrypt the message before sending.

Policy-based email security solutions need to work with the various types of mobile devices that are proliferated within most organizations. The best approach is to scan emails at the gateway to assure all emails are checked whether they originate from a desktop or a mobile device.

Training: Employee training and awareness programs are as important as these technology interventions

About Proficio

Proficio is a leading Managed Security Service Provider (MSSP). We are changing the way organizations meet their IT security and compliance goals by providing the most advanced cloud-based solutions to monitor and scan critical assets without the need for added headcount or costly software and hardware systems.

Our customers value our insight, experience and unrelenting passion for defending their networks and applications from cyber attacks. Proficio has worked extensively with healthcare providers and their partners that process or store Protected Health Information (PHI).

Proficio's ProSOC is a Security Operations Center (SOC) subscription service that logs, monitors and analyzes your organization's security events. ProSOC helps organizations address critical security and compliance needs, minimize business risk, and reduce costs.

ProSOC includes:

- Advanced SIEM technology and log management
- Full SIEM management, configuration and customization
- 24x7 continuous monitoring and analysis by certified Security Analysts
- Rapid response to critical security incidents
- Advanced protection against both perimeter and insider threats
- Web portal with easy-to-use dashboards and comprehensive reporting
- Compliance reporting and log retention for HIPAA, PCI, SOX, and others
- Full security device management services including configuring, tuning and patching firewalls, NGFWs, IDS/IPS, and WAFs

Proficio's ProSCAN is a fully automated scanning service providing continuous protection against the latest security threats without the cost of software or hardware, or hiring additional in-house security experts.

ProSCAN is powered by QualysGuard and includes:

- Vulnerability Management
- Asset Discovery and Tagging
- Web Application Scanning
- PCI Scanning
- Policy Compliance Management
- Easy to use web portal, intuitive dashboards and reporting

Proficio provides comprehensive security assessment consulting services including:

- Vulnerability Assessments
- Penetration Testing
- Social Engineering
- Application Assessments

For more information see www.proficio.com or call us at 800-779-5042.

Proficio Headquarters
1555 Faraday Avenue
Carlsbad CA 92008
USA+1-800-779-5042
www.proficio.com

Proficio London
SalesForce Tower
110 Bishopsgate
London EC2N 4AY
+34 937 370 358
www.proficio.com

Proficio Barcelona
Travessera De Garcia, 11
Barcelona Spain 08021
+34 937 370 358
www.proficio.com

Proficio Singapore
15A Changi Business Park
Central 1 #03-01/02 Eightrium
Singapore 486035
+65-6996-9185
www.proficio.com

Proficio Australia and New Zealand: Level 13
135 King Street Sydney,
NSW 2000
+65-6996-9185
www.proficio.com

For a free pilot of ProSOC, please call 800.779.5042 or email freepilot@proficio.com

PROFICIO™