

# **Defense In Depth: A Comprehensive Strategy for Securing Health Care Networks**

Norman whitepaper June 2011



## Contents

Introduction.....	3
The Cost of Malware Infections and Data Breaches .....	3
Defense in Depth and Health Care Networks .....	5
Network Level Security.....	6
Endpoint Level Security .....	9
Anti-virus Endpoint Protection is Not Enough .....	10
Conclusion .....	12
About Norman.....	13
Further Information.....	13

## Introduction

The nation's healthcare system has been undergoing tremendous change over the past few years - health care plans have been moving to a managed care model, Medicare and Medicaid programs are being scrutinized in Congress, and HIPAA and HITECH initiatives are incenting health care providers to move to electronic protected health information (EPHI). The goal of these initiatives is to simplify patient records management while protecting patients' privacy by securing personally identifiable information as it travels through the healthcare system. Information security considerations are involved throughout the guidelines and play a significant role in complying with the this legislation, bringing new and complex technologies, processes and relationships into the healthcare arena.

Healthcare IT professionals require a comprehensive, multi-layer EPHI security strategy to address security issues related to HIPAA and HITECH. A successful security strategy will protect facilities against targeted attacks, prevent data loss and theft, address hospital security policies, and protect vital patient information.

Implementation of a comprehensive EPHI strategy will provide the following benefits:

- Prevent malware execution from entering facility boundaries or propagating from an internal endpoint
- Patch and remediate system and software vulnerabilities before they can be exploited to access EPHI
- Control and monitor the flow of inbound and outbound EPHI through removable media and devices
- Comply with HIPAA requirements for safeguarding the integrity and availability of EPHI
- Improve productivity of IT staff and hospital personnel
- Reduce cost of maintaining endpoint security
- Improve IT system performance

## The Cost of Malware Infections and Data Breaches

Malware is malicious software designed to gain unauthorized access to system resources, gather information that leads to loss of privacy, and/or disrupt operation of resources on a computer network; data breaches are the result of intentional or unintentional releases of secure information to an untrusted environment. Both of these security concerns can cause significant economic impacts within a health care organization, especially when they result in the the release of EPHI. Failure to secure EPHI may result in regulatory actions such as fines, and direct business loss from lawsuits, damage to reputation, and degradation of the public's trust.<sup>1</sup>

---

<sup>1</sup> <http://www.scmagazineus.com/health-care-data-security-breaches-in-the-us/article/120069/>

In February 2009, the HITECH Act included the first federally mandated data breach notification requirements. Under this act, any organization that has experienced a privacy breach affecting less than 500 people must notify the Secretary of Health and Human Services (HHS) annually. For breaches affecting more than 500 individuals, the organization must inform the affected individuals, HHS and the media. Civil penalties of \$100 to \$50,000 can be imposed per violation - up to \$1.5 million per calendar year. If the disclosure occurs in the context of an attempt to commercially exploit or maliciously harm the patient, criminal penalties of up to \$250,000 or 10 years imprisonment may be imposed.<sup>2</sup> The costs of litigation and notification of government authorities and the media can be substantial.

Consider the following examples:

- Earlier this year, the General Hospital Corporation and Massachusetts General Physicians Organization, Inc. (Mass General) agreed to pay the U.S. government \$1,000,000 to settle potential violations of the HIPAA Privacy Rule. Mass General, one of the nation's oldest and largest hospitals, signed a Resolution Agreement with HHS that requires it to develop and implement a comprehensive set of policies and procedures to safeguard the privacy of its patients. The settlement follows an extensive investigation by OCR. The incident giving rise to the agreement involved the loss of protected health information (E PHI) of 192 patients of Mass General's Infectious Disease Associates outpatient practice, including patients with HIV/AIDS. This impermissible disclosure involved the loss of documents consisting of a patient schedule containing names and medical record numbers for a group of 192 patients, and billing encounter forms containing the name, date of birth, medical record number, health insurer and policy number, diagnosis and name of providers for 66 of those patients.<sup>3</sup>
- In 2009, a virus infected over 100 computers on Alberta Health Services Edmonton's computer network, capturing E PHI from over 11,000 patients. The costs to the facility were substantial - over \$500,000 for detection and remediation activities, \$170,000 for notification, and an estimated \$1.6M in lost business.<sup>4</sup>
- Sisters of Saint Francis Health Services was sued for \$1.3 billion (or \$5,000 per claimant) over a data breach that occurred in 2006. Sisters of Saint Francis Health Services runs hospitals in Illinois and Indiana. They lost track of 260,000 records when a contractor copied patient information onto CDs, placed the CDs in a computer bag, then inadvertently returned the bag to a store with the CDs still inside.

---

<sup>2</sup> Social Security Act, 42 U.S.C. § 1320d-6.

<sup>3</sup> Health and Human Services - <http://www.hhs.gov/news/press/2011pres/02/20110224b.html>

<sup>4</sup> Arturo Perez-Reyes / Barney & Barney, Sharing EHR: problems and solutions, May 5, 2011

- Providence Health Systems agreed to reimburse the state of Oregon more than \$95,000 in costs as part of a deal to settle a nine-month investigation into the largest data breach ever reported in Oregon. Medical records of 365,000 patients, stored on computer disks and digital tape, were in a car stolen from a Providence home services employee. The data was not encrypted. The theft revived efforts to enact stronger privacy protections in Oregon and spurred some patients to back a class-action lawsuit seeking damages from Providence.<sup>5</sup>

The Ponemon Institute has calculated the costs associated with damage to reputation as a results of data breaches. The Institute found that about 6% of patients switched to a new health care provider after being informed that their personal information may have been compromised. "Data breaches can result in an estimated \$107,580 in revenue losses from patients choosing other facilities for the rest of their lives, according to the report."<sup>6</sup>

How pervasive is the problem of EPHI record security breaches? According to the same Ponemon study, nearly 1.5 million Americans were victims of medical identity theft in 2010. According to an analysis by the Health Information Trust Alliance (HITRUST), 108 entities reported security breaches in 2009, and health care companies were responsible for 11 percent of all data breach incidents in the U.S. between 2000 and 2007. Only educational institutions had a greater number of incidents / records lost during that time period.<sup>7</sup>

Given the costs associated with malware infections and data breaches, health care institutions must develop security policies that will protect their patients' information and protect their institutions' reputations. Due to the magnitude and complexity of today's malware and attacks, traditional defenses like intrusion prevention systems, firewalls, and anti-virus software are no longer an adequate defense against cybercrime. A more sophisticated 'defense in depth' strategy is now required.

## Defense in Depth and Health Care Networks

The defense in depth security approach was originally conceived by the National Security Agency (NSA), and it was developed from a military strategy meant to delay the advance of an attacker long enough for an appropriate defense to be implemented.

The basic premise of defense in depth is to use a layered approach to network security - deploy one or more layers of protection at network boundaries (firewalls, anti-virus/malware appliances, and intrusion prevention devices), and additional layers of protection at the individual computer workstations or endpoints. This defense strategy is most effective when using multiple UNIQUE defense mechanisms – such as using multiple

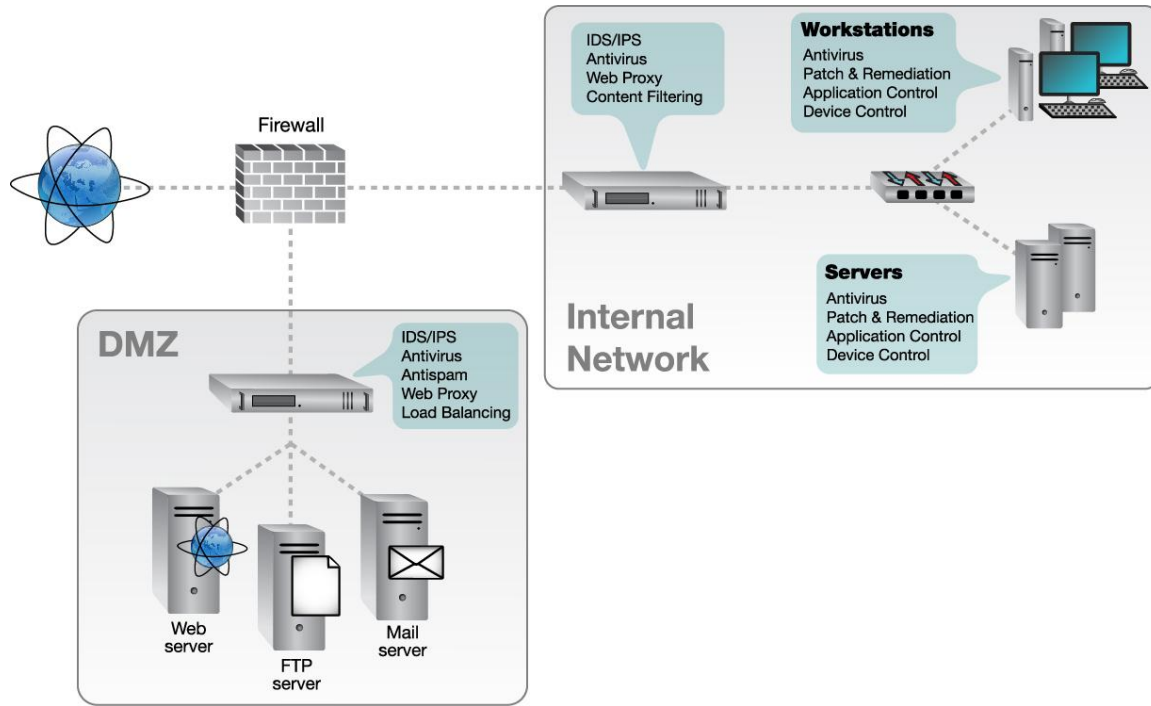
---

<sup>5</sup> Rojas-Burke, J., Providence settles data breach, *The Oregonian*, September 27, 2006

<sup>6</sup> Ponemon Institute LLC, 2009 Annual Study: Cost of a Data Breach, January 2010

<sup>7</sup> <http://www.scmagazineus.com/health-care-data-security-breaches-in-the-us/article/120069/>

vendor solutions for anti-virus control at the network level. Any gaps in one vendor’s security solution are addressed by the second vendor’s solution. This approach leverages multiple layers of defense to augment and extend protection against cyber-threats.



**Figure 1 - Layered Approach to Network Security - Protection applied at network and endpoint layers**

Defense in depth security strategies are ideally suited for the health care environment. Each layer of defense enhances a facility's protection from both external and internal security threats. The layered approach is especially valuable for protection of internal network resources that are not under direct IT control, because network level devices can identify and block incoming threats before they enter the internal network.

## Network Level Security

The first level of security to consider when implementing a defense in depth strategy is network level security. Proper attention to security at the network level will provide benefits to all downstream resources. For example, network protection appliances can be deployed at various points within the hospital network to protect network resources from hackers and viral infections. Most at risk are medical devices for which anti-virus and firewall software is not available or not under IT staff control.

Medical-device manufacturers typically prohibit hospital IT administrations from applying software updates to medical equipment regulated by the Food and Drug Administration (FDA). Many devices aren't allowed to run anti-virus software either since this might slow

down the medical application - a virus scanner could slow down a medical device like a CRT machine and alter its output. When medical equipment gets infected by malware, medical device manufacturers typically send a service team out to clean it up. This medical equipment can be protected through network level security devices that will identify and block malware before it enters the network.

Network level security devices also increase the security of computer resources that ARE under IT control - like workstations and servers. Using an anti-malware device at the network level in conjunction with a traditional anti-virus solution at the network endpoints adds up to 38% additional anti-malware protection (vs. utilizing anti-virus endpoint protection alone).<sup>8</sup>

- *Network Perimeter* - The network perimeter or edge is where Internet traffic enters and exits the health care institution's network(s). Various types of protection can be deployed, including malware protection, spam filtering, content filtering, network firewalls, and intrusion detection and prevention.

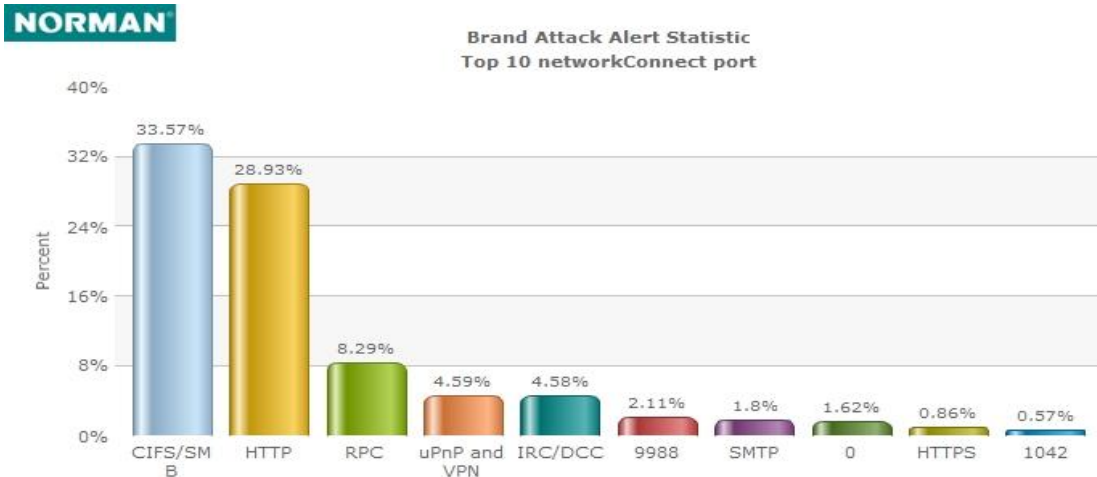
The network perimeter is often protected by Unified Threat Management (UTM) technology. This solution is typically deployed as a network appliance, and it combines multiple security functions into a single solution with a unified management interface. These devices are especially valuable at the edge of the internal network where most external 'brute force' attacks are going to occur.

UTM solutions are a critical component of network level security, and they need to be implemented carefully. For example, network firewalls must be configured so that they do not allow unnecessary protocols to pass through to the internal network, or the perimeter of the health care facility's network will be open to attack through open firewall ports. Care should also be taken when using a UTM's anti-malware capabilities - implementing so many security functions can compromise throughput, especially when the device's anti-virus and malware analysis is file-based and proxy-based. Reduced throughput will cause network congestion, slow delivery of email, and slow responsiveness when accessing Internet resources. In these cases, security officers often deploy dedicated anti-virus devices to offload some of the processing to dedicated hardware.

Additionally, the anti-virus analysis of many UTMs is applied only to Internet-based protocols like http, ftp, and smtp. Dedicated anti-malware solutions also analyze Windows-based protocols like CIFS and SMB, which represent a significant vector for both internal and external malware attacks, especially in health care networks where a great deal of data is often stored on Windows file systems.

---

<sup>8</sup> NSSLABs, Norman Network Protection (NNP) Network Anti-Malware Assessment: Q2 2010



**Figure 2 - Malware Attacks by Protocol - Largely CIFS/SMB, HTTP, and RPC**

In some cases, security personnel may also choose to deploy an anti-malware appliance from a different security vendor in-line with the UTM to provide a second analysis vector on incoming data packets - this is another element of a defense in depth security strategy.

- Segmented Networks* - Large internal networks are often organized into groups of smaller networks, either through physical network topology or through VLANs. This type of network topology reduces congestion and improves network performance by reducing the amount of traffic flowing through any one network segment. Segmented networks also provide a high level of security - broadcast traffic is contained within each local network, and network segments can be quickly isolated in the case of a security breach.

Steve Wexler, chief biomedical engineer at the Dept. of Veterans Affairs Health Administration division, has applied the concept of segmented networks to the challenge of securing unpatched medical equipment. He knows that unpatched equipment sitting on LANs is vulnerable to computer worms and viruses. As a response to this situation, Wexler worked with network engineers at the VA to craft a plan for securing the VA hospitals' networks.

This plan is described in the "[Dept. of Veterans Affairs Medical Device Isolation Architecture Guide](#)",<sup>9 10</sup> which directs IT staff to isolate medical equipment into separate VLANs.

<sup>9</sup> When medical-device equipment gets sick, [Ellen Messmer](#), NetworkWorld.com, 07/19/04

<sup>10</sup> [http://www.nwfusion.com/news/2004/VA\\_VLAN\\_Guide\\_040430.pdf](http://www.nwfusion.com/news/2004/VA_VLAN_Guide_040430.pdf)

Corporate health care IT professionals can leverage this strategy within their own networks, creating subnets for different categories of network devices and securing these subnets with network protection devices.

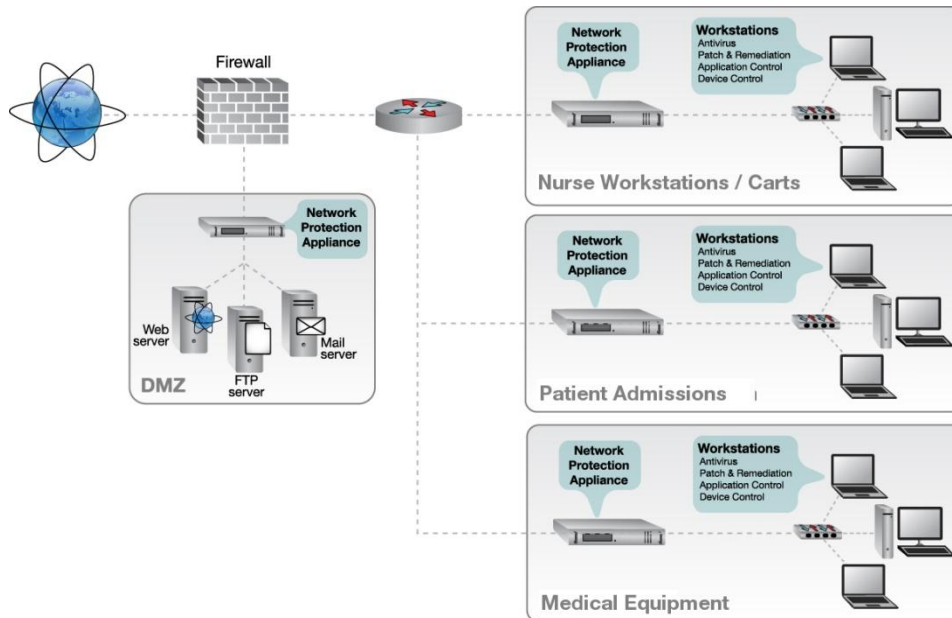


Figure 3 - Network Subnets in Health Care Facility

For example, high risk portions of the network like nurse's carts and in-room patient systems can be isolated into their own network subnets, so activities on these resources are confined to a single network segment. Vendor-managed medical equipment can be placed in a separate network segment. Each network segment can be protected with a dedicated network level security appliance to prevent viruses and malware from crossing network boundaries, and subnets can be physically isolated in the event of a serious malware infection.

## Endpoint Level Security

An effective security infrastructure must protect all network endpoints (servers, workstations, et al.) from cyber attack. These network resources are typically secured by installing anti-virus software and enabling a firewall at each endpoint.

The anti-virus software is used to prevent, detect, and remove malware (including computer viruses, computer worms, trojan horses, spyware and adware). There are a number of strategies that can be employed by an anti-virus solution:

- *Signature-based detection* - This strategy involves searching for known patterns of data within executable code. These patterns are regularly updated by the anti-virus company's research team. It is critical that all endpoints with anti-virus software

receive updated signature files regularly, since these signature files serve as the first line of defense when identifying malware.

- *Heuristic detection* - This strategy is used to identify new malware for which no signature is known. The anti-virus software identifies new viruses or variants of existing viruses by looking for patterns that are similar to those of known malicious code, or slight variations of such code.
- *SandBox detection and analysis* - This strategy executes unknown files in a protected environment and analyzes the results of that execution to see if the files trigger any malicious actions in the host environment. Sandbox solutions can identify new and undiscovered malicious code that may pass through signature-based and heuristic detection methods and stop the code before it damages computer networks and compromises confidential data.

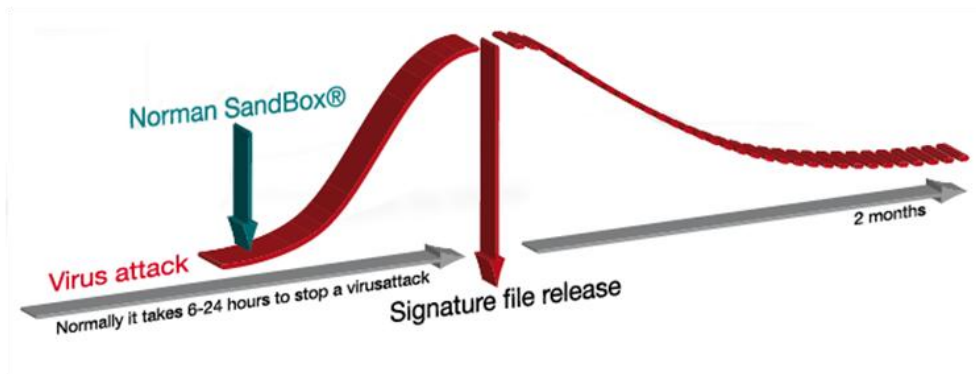


Figure 4 - SandBox Value - Malicious code identified through behavior profile before a signature file can be created

All anti-virus solutions will provide some level of protection for the network endpoints, but the best anti-virus solutions use a combination of all three techniques to protect endpoints from infection. Security personnel should periodically evaluate their anti-virus solutions to ensure that they are leveraging a solution with multiple layers of defense.

## Anti-virus Endpoint Protection is Not Enough

- Anti-virus software is a critical component of endpoint security, and security personnel must ensure that the software is installed on every server and workstation on their networks. Endpoints with outdated virus definition files are a security risk, so procedures should be put in place to ensure that all endpoints are regularly updated with new virus definition files. Once a comprehensive anti-virus plan has been deployed, a more comprehensive strategy of endpoint security should be considered – one that ensures all endpoints are kept secure through application of regular system/application patches, and monitoring of associated applications and devices. Patch and Remediation Software - Over 90% of cyber-attacks exploit known

security flaws for which remediation is available<sup>11</sup>. For example, for months the Conficker worm continued to spread to millions of computers worldwide through a security hole in Windows Server Service, despite Microsoft publishing a patch for this vulnerability.

In order for network endpoints to be completely secure, security personnel must know what software is installed and operating on each endpoint. They must further ensure that the software and operating systems of every endpoint are regularly patched to eliminate attack vectors which could be utilized by cybercriminals to compromise the resource. When properly implemented, patch and remediation solutions ensure that system and software vulnerabilities are patched before they can be exploited to access EPHI.

A comprehensive patch and remediation solution should have vulnerability auditing capabilities and remediation, and it should support all major operating systems (including Microsoft Windows, Linux, MacOS, Sun Solaris and HP) so that risk can be managed for all systems from a single operating console. The solution should have the ability to patch popular applications from vendors like Microsoft, Adobe, and Apple, and patch custom applications through a straightforward and intuitive interface. Norman Patch and Remediation is one such solution; it streamlines patch management across heterogeneous environments, provides visibility into real-time patch status and overall security posture, and reduces operational costs by centralizing operating system and application patching and remediation activities.

- *Application Control Software* - One aspect of endpoint security that is often ignored is application usage. By implementing a "whitelist" approach to managing application usage, security personnel can define which applications are permitted on the health care institution's network through user and/or machine-specific policy rules. Execution of unknown or malicious code is prevented because only authorized applications are allowed to run on nurse workstations, medical equipment, and mission critical servers.

A comprehensive application control solution should automatically determine what applications are in use throughout the network endpoints, enforce application usage policies across the entire network, and prove HIPAA compliance by providing a detailed audit trail of all application execution attempts. Such a solution should implement endpoint agents that are tamper-proof and protected against unauthorized removal.

---

<sup>11</sup> Gartner Research report, May 2002.

Application control solutions help to ensure that EPHI is not intentionally or accidentally released through unauthorized applications and they improve the productivity of facility personnel by ensuring that they are not using unauthorized applications during work hours. These solutions also lower desktop and server maintenance costs by eliminating the support and performance issues associated with managing unauthorized and illegal software.

- *Device Control Software* - Device control solutions are a critical component of a comprehensive defense in depth approach to network security. This software protects networks from internal threats like data theft by enforcing which removable media are allowed in the facility's network, and controlling the data that is copied to and from the network through policy-enforced encryption. This ensures that any EPHI is unreadable if it falls into the wrong hands. This is especially important in health care environments, where many documented HIPAA violations involve lost or stolen data that was not encrypted.

Device control solutions should demonstrate HIPAA compliance by providing a detailed audit trail of all device mounts, tracking data that is copied to and from removable devices and by controlling what data is allowed to be copied to a device at the file level.

Device control solutions ensure that the flow of inbound and outbound EPHI is controlled and monitored, and they assist in safeguarding the integrity and availability of EPHI. As with application control solutions, all data transfers must be logged for security and compliance reporting, and endpoint agents must be tamper-proof and protected against unauthorized removal.

## Conclusion

A defense in depth approach to network security will provide the most comprehensive protection against malware threats and other forms of cyber-crime. Security architectures with multiple layers of protection from multiple vendors provide the best protection, especially when deployed at multiple levels in the network. Likewise, a multi-layer endpoint management strategy with anti-virus, patch, remediation, and application and device controls will provide comprehensive protection at network endpoints.

A defense in depth architecture will also provide security teams with many of the reports necessary to demonstrate compliance with HIPAA/HITECH, PCI-DSS, and other federal and state laws and regulations that penalize institutions when they do not adequately protect the personal data on their networks.

Under the authority of the HITECH Act, the US Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) require practices to periodically assess and update their data privacy and security policies and procedures and train all staff accordingly. Therefore, security professionals are encouraged to review their facilities' security implementations periodically to identify areas of vulnerability and implement 'defense in depth' network strategies where appropriate to ensure that their network resources are adequately protected.

## About Norman

Norman is a world leader and pioneer in proactive IT security solutions and forensic malware analysis tools. Norman and their partners can offer the depth and breadth of solutions to assist educational institutions in enhancing their security defenses without risking vendor lock-in. Norman's comprehensive portfolio includes patch and remediation, device control, application control, network security, and proactive malware detection (endpoint, server, mail server or gateway) as well as advanced malware analysis tools.

Norman is recognized as a leading authority in proactive anti-malware technology, with respected security companies including MessageLabs (Symantec), eEye Digital Security and Microsoft among others utilizing Norman's technology to help protect their customers.

## Further Information

For further information and advice on Defense in Depth please contact:

### **Norman Data Defense Systems (US)**

9302 Lee Highway, Suite 950A

Fairfax, VA 22031

Tel: 703-279-6647

E-mail: [sales.us@norman.com](mailto:sales.us@norman.com)



[www.norman.com](http://www.norman.com)