FROST & SULLIVAN

SHAREPOINT IN HEALTHCARE
Collaboration and Information Sharing in a Secure Environment

A Frost & Sullivan White Paper
Prepared by Robert Ayoub, CISSP
and Martha Valazquez

TABLE OF CONTENTS

INTRODUCTION

The March 2010 signing of the National Healthcare Bill signals a new area of change for the healthcare system in the U.S. Hospitals in particular are set to be significantly affected by these new regulations as hospitals are at the center of an ecosystem of affiliated physicians, labs, and others involved in both the provisioning of care and the collection of vast amounts of information from patients. Besides the changes in coverage and insurance, a variety of technology initiatives are mandated by new regulations. Hospitals will soon be required to provide communication and collaboration platforms that allow seamless integration among the various stakeholders. These changes in information flows, along with an explosion of digital content that needs to be stored and shared, are driving a need for a secure IT platform through which hospitals can support collaboration and information exchange.

The move toward more patient-centric care and more decentralized monitoring means providers, patients and payers need to access information that originates outside the hospital setting. The trends toward personalized medicine, prevention and wellness mean stakeholders need to connect together information from various points within the healthcare value chain from providers, laboratories, payer, and patient, and, in the future, even information on diet, purchases and training regimens and results. The more this private information is opened to outside entities, the greater the chance that malicious content may permeate through these systems or leak pertinent data either intentionally or accidently.

Microsoft SharePoint is Microsoft's flagship communication and collaboration platform. Due to SharePoint's sophisticated platform, many hospitals have already begun deploying content to their various stakeholders through this system. Unfortunately, the security required by hospitals is much higher than what comes built in with SharePoint out of the box. This paper will discuss the security challenges associated with a SharePoint deployment in a hospital environment and will offer a number of industry best practices that Frost & Sullivan believes significantly reduce the exposure to risk for hospitals that are cautiously moving into a highly connected world.

INCREASING USAGE OF SHAREPOINT WITHIN THE HEALTHCARE INDUSTRY

Microsoft Office SharePoint Server is an integrated suite of collaboration capabilities that can help improve organizational effectiveness by providing comprehensive content management and enterprise search, accelerating shared business processes and facilitating information-sharing across boundaries for better business insight. Additionally, this collaboration and content management server provides IT professionals and developers with the platform and tools they need for server administration, application extensibility, and interoperability.

SharePoint is Microsoft's fastest growing product with more than 17,000 customers, 100 million seats and more than $1 billion in revenue[1]. The latest version of SharePoint, SharePoint 2010, allows the collaboration and unification of an organization's employees,

[1] Microsoft (June 6, 2008). Microsoft's Fastest Growing Product Ever SharePoint 2007

customers and other outside partners. Now more than ever, the ability to communicate over blogs and communities is advancing quickly, creating the need for organizations to abide by the demands of new and updated technology. SharePoint allows for businesses to facilitate and collaborate in an effective and cost-reducing manner. As an integrated solution, SharePoint offers organizations the ability to communicate across their intranet, extranet and Internet sites.

As the demand to shift to a modern healthcare system arises, the use of SharePoint has increased dramatically within the healthcare industry. The need to provide quality patient care while reducing costs is the most significant challenge for the healthcare industry in 2010. Hospitals have more demands for creating a platform for collaboration with care providers and provide information and interactions with patients, providers, physicians, and employees. Utilizing SharePoint gives hospitals the ability to share confidential health records and pertinent information, improving the quality of patent care. In addition, the shift to a more modern healthcare system requires integrated platforms to track and improve clinical outcomes, creating simpler administration processes and reducing expenses. Furthermore, an organization's overall efficiency and productivity can increase dramatically as Web-based capabilities such as wikis, portals and blogs help organizations share best practices internally and communicate more efficiently with its customers and patients.

SECURITY CHALLENGES POSED BY SHAREPOINT FOR A HEALTHCARE PROVIDER

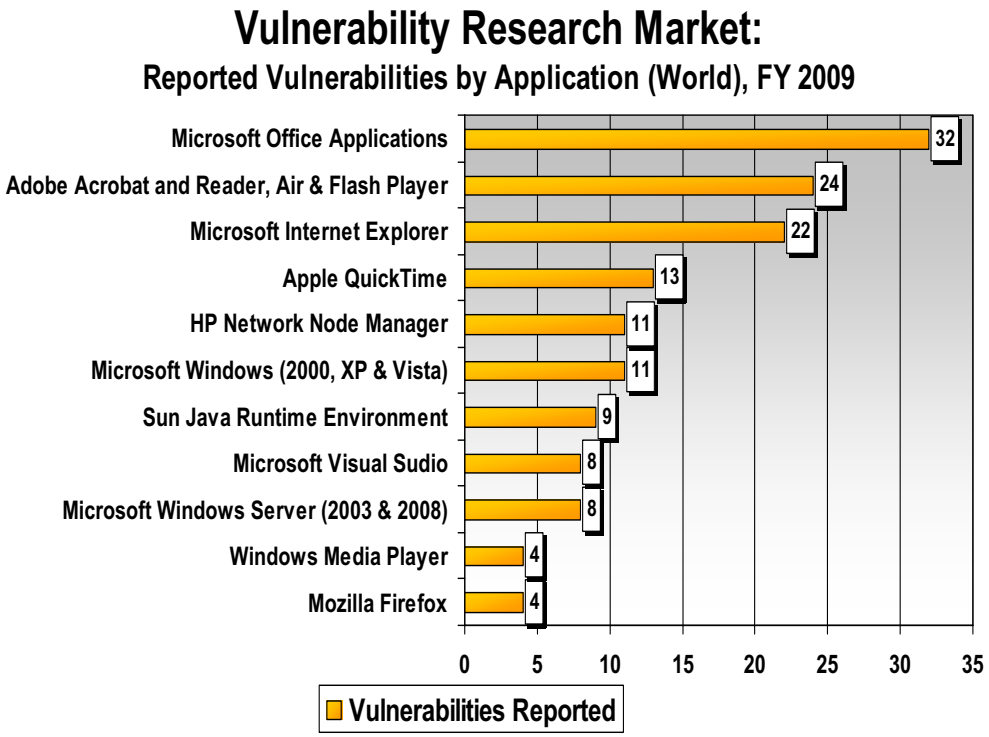
There was a time where disruption was the key goal of hackers, and hospitals were not seen as valuable targets. Cyber criminals in 2010 are not interested in causing a nuisance to corporate networks but use attacks as a means to gain financial gain. In 2010, the personal information collected by hospitals can fetch a significant sum of money on the black market, making hospitals a highly coveted target. The threats are more complex, and cyber criminals continue to improve their techniques. As threats become more malicious, IT administrators must address the challenges that come from malware entering the network. Unfortunately, there are numerous challenges today that make securing the network a daunting task.

The Changing Security Threat

The original model of network security was focused on protecting the network from the outside using firewalls and other traditional security devices. With the popularity of social media, including blogging and the use of wikis, and the requirement to provide easy access to data to partners and patients, the threat increases significantly. The modern threat can be a link that directs users to a malicious Web site or attachments embedded in a blog post with malicious code. Malware can then exploit vulnerabilities in applications and download malicious programs, such as key loggers, to steal usernames, passwords and private data. Unfortunately, the most common applications and file formats are the ones with the greatest chance of exploit. Figure 1 shows that business applications are currently targeted more than any other application[2]. Microsoft Office applications, Adobe Acrobat, Air and Reader, and Microsoft Internet Explorer had the most vulnerabilities reported against them in 2009.

[2] Frost & Sullivan FY 2009 – World Vulnerability Research Tracker, March (2010)

Figure 1 – Top Targeted Applications in 2009



Maintaining Compliance and Regulations

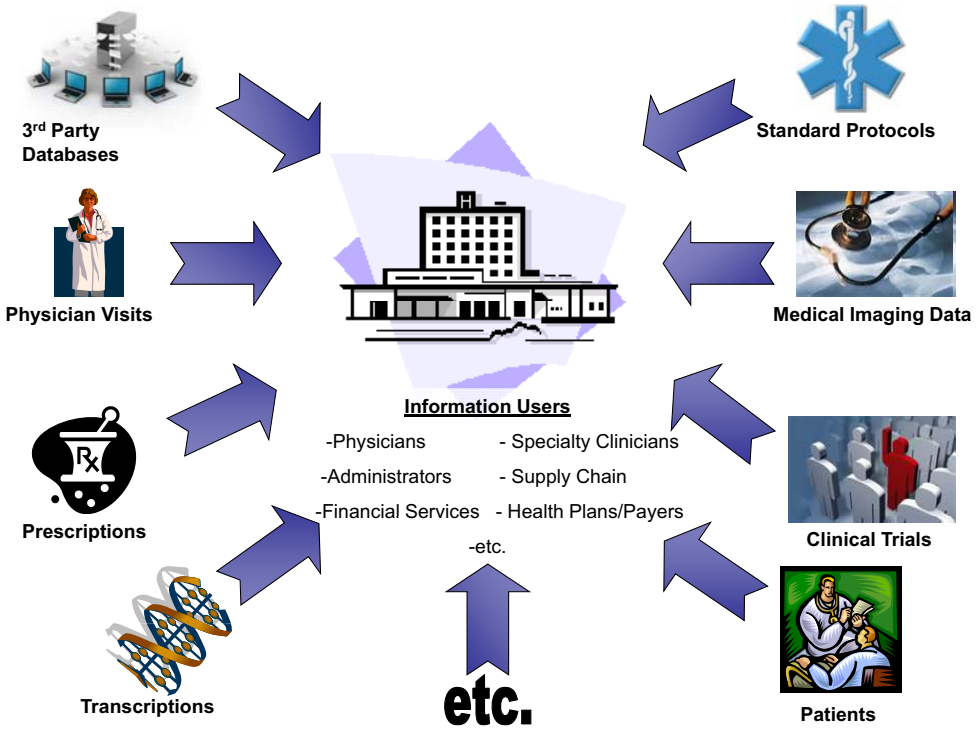
Embracing new technologies to improve the quality, the flow, and the safety of patient information is a critical issue for hospitals. Government regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act are already helping to guide hospitals in the proper implementation of new technologies. HIPAA was created to guarantee patient protection and privacy; HITECH contains incentives related to health care technology and how information is flowed through an infrastructure. It contains specific incentives designed to accelerate the adoption of electronic health record (EHR) systems among providers. The adoption of electronic health records is expected to increase the amount of security required under HIPAA and increases the potential legal liability and fees for not remaining within compliance.

Increasing Usage of Collaboration Between Patients, Employees and Outside Networks

Another challenge within the healthcare industry results from the increased expectation of collaboration from patients, employees and outside networks. Recent trends in healthcare have led to a proliferation of healthcare content, and modern healthcare depends upon the reliable, rapid and secure exchange of this information throughout a large healthcare organization. The criticality of this information, and the fact that it needs to be available to different stakeholders throughout the hospital as well as to others in the healthcare value chain outside the hospital, make a shared platform essential to effective hospital operations.

To adhere to evidence-based medicine, information needs to be consolidated from diverse sources such as third-party databases, standard protocols, physician visits, medical imaging data, clinical trials, literature references, transcriptions, prescriptions written, etc. In addition, the information needs to be viewed and vetted by various individuals, including primary care physicians, specialty clinicians, administrative personnel, employers, financial services, and claims processors to collaborate to determine appropriate care protocols, medication administration and standard operating procedures. There is a need for a collaborative workspace that can enable distributed individuals and teams to work together more efficiently and effectively toward enhancing their existing systems.

Figure 2 - Interactions between the Hospital and Outside Parties



In addition to increased information exchange between healthcare providers, there is also an increase in information exchange between hospitals and their patients. The shift toward more preventative care means ongoing monitoring and outreach to push information and treatment out to patients, and to bring information in from patients. Hospitals are using Web-based platforms for these interactions, as well as expanding the content they are providing to patients prior to arrival at the hospital, during treatment, and as follow ups to various procedures or medications that have been provided.

Increase in Mobile Solutions

The increase in mobile employees in the healthcare industry places the endpoint at risk. The use of mobile devices – tablets, laptops and even smartphones – are commonplace in the modern hospital, and the need to secure data from the Internet all the way to the

endpoint is the key concern today. Mobile employees increase productivity and improve patient care by allowing data entry remotely. Mobile connectivity is also a key strategy for many CIOs. CIOs are increasingly interested in implementing mobile applications and wireless connections within hospitals. In addition, security remains a top concern for these mobile devices contacting to the network by individual doctors, employees, and other third-party vendors. As this remains a top concern, the need to protect patient data will increasingly be of importance.

INDUSTRY BEST PRACTICES ADDRESSING SHAREPOINT SECURITY

While the current healthcare environment is improving collaboration and communication through the utilization of SharePoint, the risk to personal data and the chance of infection from viruses or malware increases. As this becomes significant for the amount of people utilizing the environment, it is advised that several recommendations should be implemented.

Implement Server Protection

While addressing these challenges, a healthcare system should be well aware of securing SharePoint at all various levels of protection, such as at the repository, portals and other file-based servers. Implementing anti-malware at the SQL server database allows for the ability to scan infected files as well as perform updated protection.

The back-end database is the critical link between the SharePoint server and all the other data sources in the hospital. The protection around this database must be up-to-date at all times and must secure protection from the latest threats as they emerge.

Ensure Protection from Zero-Day Attacks

Even diligent application of patches can allow gaps in protection for the server. The SharePoint portal can become a source of malicious and inappropriate content. A zero-day attack can compromise the server and allow access to identity information leading to reputation damage and fines.

Scan All Content as it is Placed on the Portal

With more open access to a portal, it is imperative that any links or content posted to the public be scanned for both appropriateness and to ensure that the link is not malicious – either intentionally or through mistyping. As hospitals encourage patients to engage in discussion forums, wikis and blogs pose the use of inappropriate language such as pornography, violence or racism. Keyword scanning is an additional layer of defense that will enable protection from possible malware. It also enables protection from tasteless information being placed within the portal. By also utilizing the scanning for inappropriate keywords, this will keep malicious sites away from discussion forums, hence providing an effective productive solution for healthcare providers.

By implementing a content-aware solution at the portal, a hospital can ensure that all content is appropriate. By implementing a data leakage prevention (DLP) solution on the portal, a hospital can control and monitor the access of data across the hospital infrastructure.

Protection Strategy:

1) Secure the Server

2) Protect Against Zero-Day Attacks

3) Secure SharePoint

THE TREND MICRO PORTALPROTECT FOR MICROSOFT SHAREPOINT

Frost & Sullivan believes the Trend Micro PortalProtect addresses many of the business challenges associated with the shift toward the modern healthcare system by offering a solution that extends protection to not only repositories but also to team sites, intranet, extranet portals, wikis and blogs. Trend Micro PortalProtect includes key components that can be centrally managed while reducing administration and optimizing performance. PortalProtect secures against threats received from infected files, which may enter through repositories, wikis or blogs. Some of the benefits that an organization can gain from using PortalProtect are detailed below.

Leading Advanced Threat Protection

PortalProtect offers protection from file sharing and real-time protection against Web 2.0 threats utilizing Trend Micro's Smart Protection Network, a next-generation cloud-client content security infrastructure designed to protect customers from Web threats, such as data stealing malware. The solution offers threat protection against viruses, worms, Trojans, and malicious links, and includes content filtering to prevent the loss of data and theft. Through this comprehensive protection, PortalProtect protects from infected files entering SharePoint and Web-based malware. Through its content filtering solution, high-risk or non-productive files are filtered, even if they are embedded objects like mp3 files in Word documents. It includes predefined polices to scan for objectionable content such as racist words or foul language. The Web content filtering includes real-time protection from malicious links embedded in files, Web content, blogs, wikis, and discussion forums. Predefined regular expressions allow for filtering of personal identifiable information, thereby preventing any personal data loss.

CONCLUSION

Information exchange and interaction are critical to the modern hospital environment. Care providers are looking at a future reimbursement structure that is based on measuring outcomes. Since patient treatment often originates in physician offices outside the hospital and follow-up tracking of the success of treatment occurs in these same offices, hospitals and these affiliated physicians need a platform for information exchange. Thus far, the Microsoft SharePoint platform has proven to be a solid stepping stone for hospitals taking their first steps into collaboration and information sharing.

Unfortunately, the highly financially driven threat environment and increasing regulation means that the healthcare industry has numerous challenges lying ahead to deliver a secure SharePoint infrastructure. Frost & Sullivan believes that Trend Micro's PortalProtect addresses many of these challenges and helps healthcare organizations to implement the necessary industry best practices to achieve regulatory compliance and protect against the changing threats in today's quickly evolving security landscape.

CONTACT US

Silicon Valley
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost
myfrost@frost.com
http://www.frost.com

Auckland
Bangkok
Beijing
Bengaluru
Bogotá
Buenos Aires
Cape Town
Chennai
Colombo
Delhi / NCR
Dhaka
Dubai
Frankfurt
Hong Kong
Istanbul
Jakarta
Kolkata
Kuala Lumpur
London
Mexico City
Milan
Moscow
Mumbai
Manhattan
Oxford
Paris
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Silicon Valley
Singapore
Sophia Antipolis
Sydney
Taipei
Tel Aviv
Tokyo
Toronto
Warsaw

ABOUT FROST & SULLIVAN

Based in Mountain View, California, Frost & Sullivan is a global leader in strategic growth consulting. This White Paper is part of Frost & Sullivan's ongoing strategic research into the Information Technology industries. Frost & Sullivan regularly publishes strategic analyses of the major markets for products that encompass storage, management, and security of data. Frost & Sullivan also provides custom growth consulting to a variety of national and international companies.