The security needs of healthcare organizations are growing with the implementation of healthcare reform, but providers continue to be of two minds when it comes to investing in security. Either they do not fully appreciate the real risk of cyberthreats, or they think it is cheaper to pay the fines and other associated costs than it is to invest in a comprehensive security strategy. The threshold for how long healthcare organizations can ignore security is getting lower as threats are increasing, the penalties are getting stiffer, and fines continue to increase. Healthcare reform and new reimbursement models require complex IT infrastructure, which needs to be reliable and secure and built on an extensible platform that addresses today's most pressing needs and will support future technology investments. Key considerations for a security environment that meets today's need for reliability and can withstand the onslaught of increasingly sophisticated cyberthreats are:

- **Prioritize security infrastructure.** Breach economics present a dire situation for affected hospitals. In addition to the public relations challenges and loss of patients and public trust, there are the high costs associated with remediation, notification costs that run approximately $200 per record, plus the risk of fines and lawsuits. These costs can run in the millions, if not billions, of dollars. A comprehensive risk analysis should be all inclusive and encompass all devices and device types, including medical devices, photocopiers, and HVAC and other operational systems.

- **Invest intelligently.** Hospitals and health systems should select security solutions that not only allow them to meet current security requirements but also offer extensible functionality to support a growing IT infrastructure, new devices and applications, and threats as they arise. Disaster recovery (DR) and business continuity (BC) can be considered concurrently as complementary technology investments.

- **Make security a business priority.** Healthcare organizations need to consider how they will continue to operate in the event of a security incident. They must understand how a security incident affects not only the technical and operational aspects of the organization but also the larger business in the context of their compliance strategy. Reactive security measures will not be effective in the long run. Healthcare organizations must elevate security to an executive and strategic level to ensure that infrastructure and information security is given the attention it deserves.
IN THIS WHITE PAPER

This IDC Health Insights white paper is sponsored by Symantec and examines security issues and challenges for providers in the current environment. This white paper is based on briefings with Symantec as well as IDC Health Insights’ security and compliance research. The objective of this white paper is to educate healthcare organizations about cybersecurity risks and offer guidance on how to mitigate the risk of a cyberattack.

SITUATIONAL OVERVIEW

Today's healthcare organizations are at greater risk for a cyberattack than ever before. Patient information was once available only in paper form and as a single copy of a physical chart, but it is now readily available across the enterprise and accessible by a wide range of devices, including mobile devices. The proliferation of portable and mobile devices from laptops and notebooks to smartphones and tablets has further increased the risk of a security breach. The most common data breach reported on the U.S. Department of Health and Human Services Web site that reports breaches affecting 500 or more individuals is the loss or theft of laptops and mobile devices.

In addition to security and breach risks to information, we need to understand the risks for the IT infrastructure and the operational and clinical care implications of a security incident. In today's information-driven world, access from anywhere at any time is critical and expected by clinicians. Infrastructure incidents and disruptions affect care delivery, operations and finances, staff morale, and potentially even patient lives. Being able to reliably and efficiently detect, protect against, remediate, and recover from security incidents is paramount to an industry like healthcare.

Key Threats and Drivers

Healthcare organizations are more susceptible to being hacked by cybercriminals, in part because they perceive that healthcare organizations are soft targets because of their reputation of poor security relative to organizations in other industries. Also, more sensitive health information is available today than ever before in an electronic format as a result of the following drivers:

- $20 billion in incentive payments under the American Recovery and Reinvestment Act (ARRA) to deploy electronic health records (EHRs) on tight timelines has resulted in rapid application and infrastructure implementations, with insufficient planning and hardening to ensure security.
- An aging population with more chronic conditions is producing more data and requires greater care coordination and population health management capabilities; as more data is shared between care providers in the community, the potential risk of breaches during data transmission has risen.
- Evolving care delivery and reimbursement models defined by the Patient Protection and Affordable Care Act (PPACA) require greater data aggregation for analytics and health information exchange for clinical collaboration across the enterprise, increasing risk as data pools and numbers of users grow.
- New diagnostic methods, such as three-dimensional imaging or the analysis of genomic data, are resulting in a data volume explosion, requiring rapid infrastructure expansion.
Healthcare providers often believe their industry is at low risk for malicious attacks, yet healthcare databases aggregate valuable financial, insurance, and demographic data that is increasingly targeted by malicious intruders who seek to commit both financial and healthcare identity theft. In fact, healthcare identity theft is the leading form of identity theft according to the Identity Theft Resource Center. According to IDC Health Insights' 2014 Cross Industry Cyber Threat Survey, healthcare organizations have experienced numerous — and successful — cyberattacks over the past 12 months (see Figure 1); 37% of these attacks were successful. More than half of the respondents (53%) indicated it took more than a week to identify the threat, and more than 8% of the healthcare organizations did not understand the root cause of the attack for up to six months.

As in other industries, we are seeing an increase of targeted and highly sophisticated attacks on healthcare organizations, no matter their size, location, or role in the healthcare ecosystem. Patient data in small, rural hospitals is as much at risk as research data in large academic medical centers.

**FIGURE 1**

**Healthcare Cyberattacks: Number of Attacks in the Past 12 Months**

Q. How many cyberattacks did your company experience in the past 12 months?

1. More than 10 (39.4%)
2. 1 to 3 (35.1%)
3. 4 to 5 (16.0%)
4. 6 to 10 (9.6%)

n = 94

Source: IDC Health Insights' Cross Industry Cyber Threat Survey, May 2014

To protect themselves, leading healthcare organizations are beginning to place greater emphasis on security. According to IDC's 2014 Global Technology and Industry Research Organization IT Survey, security and risk management technologies were the second top IT initiative behind mobile technologies (which actually include significant security technology component on its own). In 2013, security and risk management technologies were the number 1 IT initiative. Nearly two-thirds (62.8%) of IDC Health Insights' 2014 Cross Industry Cyber Threat Survey healthcare respondents reported that security budgets have increased over the past three years.
An Integrated Security Platform Approach

Healthcare organizations need to think about security differently than they have in the past. No longer can they install a series of disparate point solutions in a patchwork fashion and expect to adequately protect their IT infrastructure and data assets. The first step toward developing an integrated security strategy is to have a clearly articulated business strategy. The IT strategy then evolves from the business strategy. The privacy and security strategy should be aligned with both the business strategy and the IT strategy. In essence, this combination of business and IT strategies, along with the privacy and security strategy, provides an integrated framework for security governance. In other words, an integrated platform approach upon which to build a comprehensive strategy to secure both infrastructure and information assets should be used. Components of a mature security strategy should include datacenter improvements, endpoint security, disaster recovery and business continuity, mobile and medical device security, and regulatory compliance.

Datacenter and Endpoint Security

Today's healthcare organizations are faced with increasingly complex infrastructure requirements in the datacenter. Changing business models and regulatory requirements are forcing IT to be more agile and responsive to end users in healthcare organizations, rolling out new IT services rapidly while optimizing and rationalizing IT operations under tight budget constraints. Infrastructure requirements include rapid deployment of servers, storage and applications, workstations and laptops, mobile devices, and analytics tools that allow providers to meet the data and technology demands of the business in a timely manner and at low cost. IT organizations also need to pay close attention to infrastructure requirements for regulatory compliance, business continuity and disaster recovery planning, and virus and malware protection. Infrastructure-wide solutions need to be considered because point solutions will not be effective in complex hybrid environments, and infrastructure configuration and continuous updating and hardening against threats need to be part of the overall security strategy for the organization. Plans should be put in place that allow providers access to electronic protected health information (ePHI) on an as-needed basis while utilizing encryption of data at rest and in motion as appropriate, role-based management of individuals with access to data, and the endpoint devices where they are allowed to access and potentially store electronic PHI.

Whether the healthcare organization's datacenter is on-premise or in the cloud, or a hybrid of approaches, datacenter security is vital to the healthcare organization's overall security strategy. Use of virtualization tools to build private cloud environments can allow IT to secure the data and applications encapsulated within the virtualized environment, in the datacenter, and on the desktop. Server virtualization can help make the datacenter more agile and provision new resources more effectively and efficiently, saving in hardware and sometimes software costs as the number of physical servers is reduced and compute capacity more fully utilized in the virtualized server environment. Desktop virtualization can also be used to allow access to applications and data on endpoint devices while keeping data secure in the datacenter, but it can be complex, and there are still security issues that need to be considered. Using virtualization well requires a learning curve for IT staff who may need new skills and capabilities to manage the virtualized environment properly. Desktop or client virtualization can be a key strategy for accomplishing the task of securing data that is presented on multiple devices and form factors while preventing the unauthorized downloading or inadvertent loss of data, but it is one of many solutions and has inherent complexity of its own. Although virtualization provides economic and segregation advantages, it also makes security management more complicated and, if not executed properly, may reduce the security posture of an environment.
Disaster Recovery and Business Continuity Strategy

Disaster recovery and business continuity has always been an important activity in healthcare, but in the past, healthcare was less automated, and DR/BC efforts focused more on physical scenarios like transfer of paper records and staff relocation should the physical plant become unusable and patients need to be evacuated. Now that IT plays a critical role in care delivery for most organizations, and mission-critical systems are no longer paper based, IT strategies for DR/BC have risen in importance. The advent of accessible, cloud-based DR/BC technology has also made comprehensive, geo-dispersed DR/BC planning feasible for more healthcare organizations, driving further interest and focus. DR/BC should be a component of the healthcare organization’s security strategy because it will allow the enterprise to operate and recover should catastrophic events, including a major cybersecurity event, occur.

Acute and ambulatory settings, as well as ancillary services, should be included in DR/BC planning and testing as part of the overall strategy. In the case of an event, staff needs to know the processes and where to go to access services (and/or plans need to be made to notify patients and staff if services will not be delivered). Cloud services and mobility can help support DR/BC efforts by making data and applications ubiquitous and more easily accessed in the event of an emergency. Thus, the DR/BC strategy must include the secure movement of information, which includes maintaining target applications, developing and testing contingency plans for bringing them up in DR facilities and remote datacenters, and making data available from the DR location in the event of an event or emergency.

Mobile Device Security

The proliferation of mobile technology used by clinicians to care for their patients is placing additional strain on the network and security infrastructure. Along with the widespread adoption of mobile technologies come the following security threats:

- Stolen/lost devices
- Inappropriate access to the enterprise network, corporate IT assets, and applications
- Data loss
- Privacy and security breaches
- Risks associated with social media and cloud storage
- Mobile malware and threats

Thus, healthcare organizations must reexamine their security strategies. Mobile security is now a requisite component of an enterprise's overall security strategy. Loss or theft of electronic devices, including mobile devices and especially laptops, is the leading cause of data breaches according to the U.S. Department of Health and Human Services "Wall of Shame" Web site that identifies breaches affecting 500 or more individuals. In 2013, 58.3% of the breaches were the result of lost or stolen devices with more than 6 million patient records exposed as a result. The increased liability for privacy and security breaches under the HIPAA Omnibus Rule, which became effective in September 2013, makes this a significant concern for healthcare C-suite executives.

Bring-your-own-device (BYOD) strategy is creating additional mobile security challenges when a device containing both personal and clinical information goes missing. Healthcare organizations will have to invest in mobile security technology such as mobile containerization that separates the employee’s applications,
data, and content (e.g., personal contact lists, email, text messages, and photos) from the healthcare organization's assets. Thus, in the event the device is lost or stolen, or the employee leaves the healthcare organization, the corporate assets can be remotely wiped from the device. Organizations that support BYOD should require employees to agree to remote locking and wiping in the event their device goes missing or they change jobs. Other concerns include the introduction of malware from employees' devices into the healthcare organization's network. This user-led trend is creating tension between users who want to use their own technology and the IT organization that wants to have control over IT resources as well as know who has access to them and how they are deployed across the organization.

**Medical Device Security**

Wired and wireless medical devices connected to the healthcare organization's network are another source of growing concern among healthcare security and patient safety professionals. Securing medical devices is inherently complex. If not properly secured, medical devices, such as bedside telemetry or implantable devices like pacemakers and insulin pumps, can be hacked or can introduce malware to the network and in extreme cases create a life-or-death situation for the individual whose medical device is hacked. Security researchers have demonstrated the ability to hack a pacemaker (Kevin Fu, 2008) and an insulin pump (Jay Radcliffe, 2011). Barnaby Jack, a New Zealand hacker, programmer, and computer security expert, demonstrated at various conferences the ability to remotely reprogram an insulin pump, which would allow him to deliver a deadly insulin dose.

Medical devices are often vulnerable because of poor security practices, such as hardcoded or default passwords, lack of system hardening, out-of-date patch level, and the absence of cybersecurity tools. According to a June 13, 2013, alert from the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), password vulnerability affects roughly 300 types of medical devices across approximately 40 vendors.

Any vulnerability in the device's software, firmware, or commercial off-the-shelf software (like the operating system) can be exploited by an attacker or is at risk of a malware outbreak — not because the device is being targeted but because of its poor security posture and exploitable vulnerability (e.g., due to poor patching). To date, the impact on patient safety and lives is only theoretical, but the possibility of a breach by exploiting vulnerable medical devices has been demonstrated in security research. Today, the bigger problem for hospitals is operational and financial as device malware infections affect or even shut down clinical operations, sometimes across entire departments.

Manufacturers of medical devices may also refuse to support them or terminate warranty if the original system configuration is changed, including hospital-applied patches to the operating system or installation of antimalware software tools. Healthcare organizations are just beginning to fully address the vulnerabilities associated with connected medical devices. Only 9.6% of respondents to IDC Health Insights' 2014 *Cross Industry Cyber Threat Survey* reported that medical device security is integrated into the enterprise security infrastructure. Most of the remainder of the respondents indicated that they were in various planning stages, including conducting a full risk assessment for medical devices (34%), identifying potential security threats (33%), and testing and verifying that medical devices are secure and free from malware (12.8%). One in 10 respondents had not yet begun to assess the potential security threats to networked medical devices. New FDA guidance on medical device security was issued in early October 2014 that may help clarify the issue of medical device security, asking manufacturers to justify security approaches, but there are still medical device vulnerabilities that have yet to be addressed.
Meeting healthcare compliance requirements is growing increasingly complex. With multimillion-dollar penalties, mounting breach costs, and risk of lawsuits, not to mention loss of reputation of the healthcare organization, too much is at stake for organizations that do not focus on obtaining and maintaining compliance. But information management and its related compliance activities are more than just the responsibility of the IT organization. Progressive healthcare organizations think beyond the technical risks of a security incident and the requisite investment in security technologies or reactive remediation efforts. Instead, healthcare organizations consider the business risk of a system failure after a security incident and look at security in the context of their compliance strategy. That is, what happens to patient care, access to mission-critical applications, or other services in the event of a systems outage after a breach? Outages can range from under 1 hour to more than 72 hours, severely impacting patient care and service levels. The majority of healthcare respondents to IDC Health Insights’ 2014 Cross Industry Cyber Threat Survey reported that the longest impact to normal business operations after a successful cyberattack was between 8 hours and 24 hours.

One of the first things healthcare organizations should do is conduct a security risk assessment of the potential vulnerabilities and threats to protected health information. In fact, HIPAA Security Rule (45 CFR 164.308) and the CMS Meaningful Use Incentives require that providers perform a security risk analysis and correct or mitigate identified deficiencies. The risk assessment should include technical risks (e.g., data, applications, interfaces, networks, and devices), physical security, and administrative safeguards including policies and procedures for safeguarding PHI, security training for all members of the workforce, and the protocols for responding to suspected or known security incidents. Risk assessments should be an ongoing process to avoid complacency when it comes to security and to minimize deviations from security processes through continual assessments and remediation efforts. They should also be comprehensive and include all devices and systems that store or transmit ePHI, including medical devices. Furthermore, cyberthreats are continually evolving, and cybercriminals are becoming more sophisticated, making it more difficult to protect the healthcare organization against nefarious attacks.

VALUE PROPOSITION: WHAT IS THE BUYING VISION FOR SECURITY?

Today’s healthcare security IT buyer has many issues to consider. Security no longer involves only a physical datacenter as data and applications proliferate on mobile and other endpoint devices throughout the community, but security budgets continue to be low relative to the total IT budget in healthcare. Historically, with limited budgets, IT security investment in healthcare has lacked a comprehensive strategy for meeting the needs of the organization. When lost laptops make the headlines, healthcare providers take measures to encrypt data on laptops; then when malicious hackers are in the news the following year, the focus moves to intrusion detection and perimeter security. But efforts rarely happen in concert, and strategic, end-to-end security infrastructure is never put in place, making the hospital perpetually vulnerable to the next security challenge. No security approach is inviolate, and breaches will always be a risk faced by healthcare organizations, but smart approaches to security infrastructure investment can help build an extensible security framework that allows smart investment of available funds and allows organizations to make the most of existing investments.
Implementing security in the healthcare organization requires a delicate balance between compliance and patient care. IT teams need to recognize the productivity challenges that may be created by security measures and keep processes as simple and self-service as possible to accommodate busy providers but still meet the requirements for the secure environment. Approaches such as virtualized desktops, tap-in/tap-out authentication, single sign-on, secure texting, and BYOD policies make it simple for clinicians to make the most of technology while helping keep the organization safe from breaches. When user-friendly security measures are built into organizational processes, security becomes a habit and less cumbersome for end users.

Obtaining and maintaining compliance can be challenging in healthcare. The pace of change and growth is relentless, and accountable care and other new business models require the implementation of new applications and infrastructure. With each new application comes the work of installing and running the application as well as provisioning the users and enabling the endpoint devices that will be involved and maintaining them over time. A comprehensive security portfolio should include tools to manage infrastructure on-premise and in the cloud, secure applications, communications and data with encryption on servers, desktops and devices, and offer business continuity and disaster recovery protection in case of breach or other event. This digital security portfolio should be implemented with an eye toward process management as a critical component to enforcement and effectiveness and also in parallel with compliance initiatives involving components of the environment that may still exist in paper on-premise or offsite. This infrastructure and the people and processes must be tested and ready and the architecture agile enough to address today’s threats but also extensible to allow organizations to add new approaches as they are developed to address evolving challenges.

**ESSENTIAL GUIDANCE**

With early healthcare IT systems in place since the 1970s, 40 years of progress has resulted in many gains in automation around the quality and delivery of care, documentation, and billing and payment, but security and privacy of patient records and data remain an issue. Healthcare organizations upgrading their security infrastructure and managing compliance face a daunting challenge. IDC Health Insights recommends that healthcare organizations consider the following actions as they build out their integrated security platform:

- **Conduct ongoing risk assessments.** Healthcare organizations should begin by examining current security challenges and existing investments with an eye toward identifying gaps and out-of-date approaches, dependencies, and potential areas of concern. While providers may need to address serious issues more immediately, a comprehensive effort to assess security vulnerabilities and develop a strategy will provide a guide to prioritizing concerns, identifying key investments, and planning a strategy for building security capabilities over time. Conducting risk assessments is not a “one and done” endeavor. Security threats are constantly evolving, and healthcare organizations should remain vigilant to ensure that their security strategy can be quickly modified to address the latest security threat.

- **Set key IT goals that lead to new levels of IT security services and new services.** The initial risk assessment should be used to prioritize security investments and to provide concrete timelines for investments and rollouts of security measures. Work with partners that understand the risk as well as budget and workflow constraints.
- **Evaluate and document the technical and business risk.** Which applications use or create ePHI and should be treated carefully? Which don’t and can be moved to the cloud and secured there with limited risk? Providers should weigh the benefits and risks of each workload and understand the risk and impact of security changes.

- **Find a trusted partner.** Look for a trusted internal expert and/or partner to facilitate the ongoing risk management process, beginning with the risk assessment. An internal IT compliance leader such as a chief compliance officer, a privacy officer, or a security officer should take responsibility for the overall security strategy and its role in the organization’s larger IT planning. This individual should be responsible for working with outside consultants and suppliers to build a security strategy and make investments; find the necessary technology, services, and expertise; and maintain a culture of sustained compliance within the organization.

- **Look for security providers with healthcare offerings, plus industry experience and expertise.** Security partners and suppliers should have a good understanding of the healthcare industry, experience with healthcare customers, and an understanding of the constraints associated with handling HIPAA-protected data and with the unique demands of healthcare applications.

- **Choose infrastructure over information security.** Many organizations make the mistake of raising alarms over the security of particular applications or data sets and specific use cases, leading to piecemeal security investments. Healthcare organizations, particularly those with very limited security budgets, should look first to secure infrastructure in order to get further with limited funding. Infrastructure should be configured to support existing applications and updated continuously when changes and new additions to the environment occur.

- **Manage security risk but don’t rule out cloud.** As with on-premise deployments, security issues need to be managed carefully but should not be a deterrent to cloud strategies. Healthcare organizations should seek business associates that are willing and have the financial wherewithal to put in place the security and policy framework needed to minimize the overall risks associated with safeguarding ePHI and to back their services contractually. The business associate should be willing to provide reasonable levels of liability that ensure the appropriate party, including its subcontractors, bears specific costs associated with a breach for which it is responsible, such as regulatory penalties, fines, and required actions, as well as follow-on legal actions by victims. Cloud service providers familiar with healthcare will understand the risks and penalties associated with HIPAA breaches, but cloud service providers with less experience in the vertical may require education. It is important that both customer and supplier have a full understanding of the breach risk and economics before entering into a relationship.

- **Require business associate agreements and healthcare-specific SLAs for cloud service providers.** Security should not be an obstacle to leveraging the cloud in the organization, if appropriate precautions are taken. Best practices for constructing SLAs with cloud service providers should include both compliance with HIPAA rules and service metrics specific to the demands of the application and end users. For many organizations, concerns about security and, more generally, the uncertainty of cloud raise significant risk challenges. Technically, many of the risks of the cloud can be managed, though not eliminated, with appropriate SLAs.

- **Focus on workflow first.** Infrastructure security work can often be done behind the scenes without affecting end users, and its unseen value to organizations presents one of the biggest challenges to attracting budget. But when IT finds it necessary to implement security measures that do affect end users, such as single sign-on or upcoming enhancements to add dual-factor authentication for electronic prescribing of controlled substances, it is key to consider end-user workflows and plan security approaches that will result in the highest possible continuity and minimize the impact on provider productivity.
- **Develop best practices related to security.** Each provider IT organization will need to experiment to determine the balance of security practices that are best suited to the needs of its staff and end users and the priorities of the organization. The transition from information to infrastructure security approaches may result in changes to staffing and service roles in the IT department, and this can take time. Responsibilities will shift, and skill requirements will be different as IT becomes more centralized and desktop support more automated, as a result of operating in a virtualized environment. The level of investment available and the approaches required will vary according to each organization's physical infrastructure, IT growth, and strategy needs, and best practices will vary with these goals.

- **Connect security to other new technology investments.** Securing the IT environment should go hand in hand with developing disaster recovery and business continuity technology and practices, ensuring a stable environment with sufficient uptime and availability, bringing new technology and applications to end users within the secure environment, and even reengineering workflows in the organization to enhance productivity. Most providers are in a battle to enhance provider productivity, and most strategies for enhancing productivity involve mobile devices and new form factors for technology, as well as implementing workflow changes with technology. Security practices need to be part of this, and tools like virtualization, persistent sessions for mobile workers, and single sign-on environments can be important parts of clinical technology productivity improvement strategies.

- **Promote security infrastructure awareness.** The pace of change in the industry, in terms of both business models and regulatory requirements, means new IT projects and upgrades are always in the mix. A growing trend that will create security issues for IT is when line-of-business buyers acquire cloud-based "as a service" solutions without the knowledge of IT. Security teams should be involved in new rollouts and changes that may require updating of the security infrastructure, even when investments are made by the line of business and not centrally by IT, to ensure the new solutions can be safely secured and comply with the organization's security policies.

- **Prepare for audits.** Providers are increasingly subject to audits of the security environment from multiple regulators or standards bodies. An ongoing compliance program should be used to prepare the organization for security audits, with documentation of security processes and procedures. Support your readiness by conducting internal security audits and specific tests.

## PARTING THOUGHTS

Healthcare organizations are experiencing ever higher numbers of security breaches as more information is available in electronic form, healthcare organizations are encouraged to share patient health information to meet the new demands of emerging care delivery and business models, and clinicians are clamoring to use their own personal devices to access health information inside and outside of the institution. These breaches range from relatively benign, unintentional security incidents to malicious attacks for nefarious reasons. Organized criminals view healthcare organizations as soft but very attractive targets because they have historically underinvested in security and hold both medical data and financial data that is valuable on the black market. A systemic approach to securing both infrastructure and information is required to protect against the wide range of security risks facing healthcare organizations today, including data loss, HIPAA privacy and security breaches, loss of reputation and consumer confidence in the event of a HIPAA breach, and lengthy outages caused by successful cyberintrusions. Healthcare organizations should think beyond essential compliance when it comes to security. The first step in developing a comprehensive security strategy is to conduct
a full risk assessment of both the technical risks and the business risks. Healthcare organizations that are not proactive about security risk being constantly in a reactive mode, paying more for remediation, subsequent fines, and notification and losing business to competitors that better protect their patients' health information.
About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world’s leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.935.4445
Twitter: @IDC
idc-insights-community.com
www.idc.com

Copyright Notice

Copyright 2014 IDC Health Insights. Reproduction without written permission is completely forbidden. External Publication of IDC Health Insights Information and Data: Any IDC Health Insights information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Health Insights Vice President. A draft of the proposed document should accompany any such request. IDC Health Insights reserves the right to deny approval of external usage for any reason.