Healthcare Information Security Today

2011 Survey Executive Summary: Safeguarding Patient Information - Unfinished Business

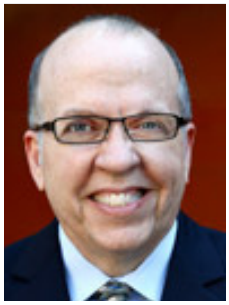
INSIDE

- Complete Survey Results
- In-Depth Analysis
- Expert Commentary

iSMG
INFORMATION SECURITY
MEDIA GROUP

Health Info Security: A Status Report

Survey Pinpoints Challenges, Highlights Action Items



Howard Anderson

The HITECH Act, a component of the economic stimulus package, is providing billions of dollars in incentives for implementing electronic health records in hopes of improving the quality of care for patients. It's also supporting the creation of health information exchanges, with a goal of ultimately enabling the national exchange of potentially life-saving information.

Healthcare organizations are making big strides in digitizing patient information. But is enough being done to protect this sensitive data? The results of the *Healthcare Information Security Today* survey are critical to understanding the changing landscape. The survey pinpoints the key privacy and security challenges and illustrates that there's still a lot of work to be done.

More than 340 major health information breaches have been reported to federal authorities since the HIPAA breach notification rule took effect in September 2009. Several big-name healthcare organizations, including UCLA Health System and Massachusetts General Hospital, have been fined for HIPAA violations.

Clearly, efforts to safeguard patient information and prevent breaches are coming up short.

The nation's chief HIPAA enforcer, Leon Rodriguez, who heads the Department of Health and Human Services' Office for Civil Rights, points out that protecting patient privacy is an important way to help ensure patients have access to care. "Very often, a patient who does not have confidence in the security of their information ... may not seek care in situations where they absolutely should," he notes.

As the nation moves toward more widespread use of electronic health records and health information exchanges, assuring patients of their privacy is essential. Without consumer confidence, EHRs and HIEs are destined to fail. And quality of care could suffer.

So what are the key challenges, and what remains to be done? The survey executive summary that follows provides answers.

Howard Anderson
Executive Editor
HealthcareInfoSecurity

Table of Contents

Healthcare Information Security Today Survey

Initial Findings

Safeguarding Patient Information: Survey Reveals Unfinished Business

So how well prepared are healthcare organizations when it comes to safeguarding sensitive patient information? The survey pinpoints shortcomings:

26% **Percentage of organizations that have yet to conduct a risk assessment, as mandated under HIPAA**

43% **Percentage that grade their ability to counter information security threats as poor, failing or in need of improvement**

43% **Percentage that have a defined information security budget**

Read on for more findings and analysis.

What is the Survey About?

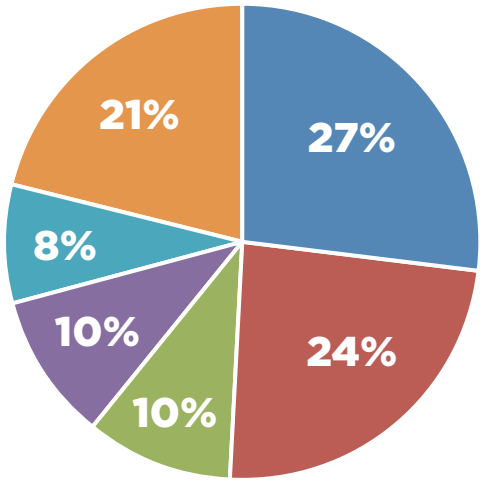
For decades, healthcare has lagged behind other industries when it comes to implementing information technology. Now that healthcare is playing catch-up, thanks, in large part, to federal funding provided by the HITECH Act, it faces the challenge of ensuring the privacy of newly digitized healthcare information.

So as hospitals, clinics and others are implementing electronic health records and health information exchanges, they're scrambling to develop robust information security measures to assure patients that their records will be protected.

HealthcareInfoSecurity conducted the *Healthcare Information Security Today* survey to provide an in-depth assessment of the effectiveness of these data protection efforts and to pinpoint areas where more work needs to be done.

The survey results are critical to understanding the challenges that hospitals, clinics and other organizations face. The survey sizes up healthcare organizations' efforts to comply with rules and regulations, including HIPAA and the HITECH Act. It investigates information security budgets, technology investment priorities and patient information protection policies. It pinpoints security threats and the ability to counter them. And it provides insights on top information security priorities for the months ahead.

What is your title?

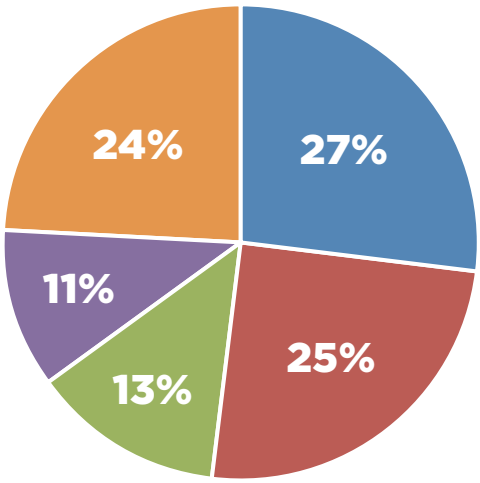


- 27% - Chief Information Security Officer or similar title
- 24% - Director/Manager of Information Technology
- 10% - Chief Information Officer/VP of Information Technology
- 10% - Chief Compliance/Risk Management Officer
- 8% - Chief Privacy Officer
- 21% - Other IT and administrative titles

The survey was developed by the editorial staff of Information Security Media Group with the help of members of the *HealthcareInfoSecurity* board of advisers, which includes leading healthcare information security and IT experts. The online survey was conducted in August and September 2011. Respondents included 175 IT security professionals and others, including chief information security officers, directors of information technology and CIOs.

These executives work at hospitals, integrated delivery systems, physician group practices, insurers and other healthcare organizations.

What type of organization do you work for?



- 27% - Hospitals
- 25% - Integrated Delivery System HQ
- 13% - Physician Group Practice/Clinic
- 11% - Health Insurer/Payer
- 24% - Other (home health, hospice, long-term care, lab, etc.).

Hot Topics

The survey unveils six hot information security topics:

1. Top Priorities. Top Investments.

Healthcare organizations still have a lot of unfinished business when it comes to information security. Topping the priority list are improving regulatory compliance and boosting security education. Top technology investments are audit logs and mobile device encryption.

2. Key Threats and Mitigation Steps

Insider threats and staff mistakes are the top security concerns, and organizations are taking a number of mitigation steps, including expanding use of encryption and implementing mobile device security strategies.

3. Compliance: Keeping Up is a Challenge

Complying with the privacy and security requirements of the HITECH Act and HIPAA is proving challenging. For many, risk assessments and breach notification planning are lagging.

4. Resources: Budget and Staffing Woes

Winning financial support for technology and staff investments is a continuing challenge, and many clinics, hospitals and other healthcare organizations lack a documented information security strategy.

5. Cloud Computing: Untested Waters

Roughly one-third of organizations are using cloud computing, with others citing concerns about security issues and HIPAA compliance.

6. Business Continuity: A Status Report

Although virtually all organizations have a business continuity plan in place, a minority update or test their plan annually.

In the pages that follow, we dive into each of these hot topics with survey results and analysis.

Experian® Data Breach Resolution on Breach Preparedness

Bob Krenek, Senior Director, Experian Data Breach Resolution

Bob Krenek

It has been 14 years since the enactment of HIPAA. Yet it is only recently that we are beginning to understand the impact and intent of what has become a wave of regulatory focus on privacy and security, especially as it pertains to an individual's protected health information (PHI). With the latest HITECH Act mandates, the healthcare industry is finding that, yes, HIPAA is here to stay. Not only that, but now covered entities and business associates need to prove that they're actually doing what their policies and procedures state. [1]

The *Healthcare Information Security Today* survey indicates that only 4 percent of healthcare organizations are highly confident in the security measures of business associates and their subcontractors. Additionally, 43 percent rank their own ability to counter external and internal security threats as failing, poor or in need of improvement.

The survey clearly reflects that healthcare organizations are aware of the urgent need to improve technology and training in order to protect PHI but still have a long way to go. Knowing this, I believe that data breaches will continue to cause problems for healthcare organizations until – and likely even after – all of today's key security challenges are addressed.

Organizations have to keep in mind that the technological aspects of data security are always changing. And, you can never completely eliminate human error. So while organizations focus on training their staff and improving their technology to help protect data, I believe a third goal also needs to be addressed: Preparing for a data breach. This means outlining exactly what steps you would take to bring things under control if one occurs.

There's a lot to lose if your organization experiences a breach of PHI. If the breach catches you off guard, you may face severe fines and reputation damage for mishandling it. Fifty-four percent of companies believe it can take 10 months to more than two years to restore their reputation following a breach of customer data. [2]

There are steps that your organization can take to help prepare for and minimize the risk associated with a data breach. Just remember, you want to AVOID LOSS:

- **Appoint a responsible party:** Every organization needs a dedicated resource to handle privacy and security issues. This person or team should implement process improvements, review noncompliance issues, initiate any investigations and assign leadership for all legal and notification efforts in the event of a breach.

- **Vet your compliance training:** Healthcare organizations need to make annual compliance training a priority. A variety of individuals require access to PHI to perform their jobs, and everyone needs to be aware of the risks associated with mishandling PHI. The more informed everyone in your organization is, the stronger your compliance efforts are.

- **Observe information:** Automated monitoring of employee and patient information will alert organizations to possible data breaches, often before they spiral out of control.

- **Instill a compliance culture:** All individuals — staff, contractors and partners — must be diligent in their compliance and alert the responsible party to processes and/or individuals who may be operating outside of privacy policies.

- **Design a long-term plan:** Develop a formalized security strategy that is flexible enough to address changing threats and legal requirements. Update it as needed.

- **Leverage response efforts:** Know in advance whom you would call for a forensic analysis of a breach as well as data breach resolution services, including consumer notification, call center support, identity theft protection and fraud resolution services for affected individuals.

- **Organize notifications:** Various state and federal laws mandate notification timelines and standards. Breach notification should occur in a timely, thorough and clear manner following the discovery of a breach. Engage a data breach resolution provider to keep your notification efforts compliant and on track.

- **Secure most vulnerable customers**: In order to mitigate the risk of new account fraud from occurring among consumers with exposed PHI, offer complimentary subscriptions for an identity theft detection, protection and fraud resolution product.

- **Sympathize with consumers:** Maintain open communication with and provide assurance to affected individuals that the situation is being professionally addressed through a robust data breach resolution program. How you handle or mishandle data breach response can help to either reduce or increase potential consumer fallout.

Data security is sure to remain an important initiative and challenge for healthcare organizations. Be sure you're prepared if your security measures are compromised and a data breach occurs.

"There's a lot to lose if your organization experiences a breach of PHI."

Other Resources

Blog

Join our conversation to learn more about breach notification, breach prevention, fraud resolution, and identity theft solutions.

http://www.experian.com/blogs/data-breach/

White Paper

Best Practices for a Healthcare Data Breach: What You Don't Know Will Cost You

http://www.experian.com/data-breach/wp-best-practices-healthcare-data-breach.html

Webinar

Preparing for a Healthcare Data Breach: What You Don't Know Will Cost You

http://www.experian.com/data-breach/data-breach-information-webinars.html

1. Risk Assessment in HITECH, Experian® Data Breach Resolution and Sinaiko Healthcare Consulting, Inc. (2010)
2. Reputation Impact of a Data Breach, Ponemon Institute (2011)

Diebold on Securing Healthcare Data

David Kennedy, Vice President and Chief Security Officer, Diebold Incorporated

David Kennedy

Healthcare is unique compared to other industries when it comes to security. That's because in healthcare, the focus is on the patient and supporting the mission of care. However, the goal is to create an environment that is open and comfortable, yet private and safe, especially as it pertains to sharing and protecting information.

In order to receive the proper care, patients must share information with their caregiver and clinicians. In doing so, they must feel confident that the information will remain secure and protected and that it is only exchanged with those directly involved in their healthcare. Because of the increase in the number of breaches involving healthcare organizations, managing the security of private, sensitive patient information is a serious concern.

The *Healthcare Information Security Today* survey confirms these concerns. But what strategies should be employed to mitigate risks, protect a healthcare organization's systems against internal and external threats and ensure compliance?

Survey respondents agree that training is a top priority. Training and improving security awareness and education for physicians, staff, executives and boards can play a key role in addressing internal threats and staff errors, which survey respondents perceived as the biggest security threats. Though damaging, insider threats may not always be deliberate and premeditated. Oftentimes, sensitive company data is unintentionally made vulnerable through the use of a variety of prevalent consumer technologies, such as instant messaging, smart phones, USB flash drives and other smart devices that have the ability to move large amounts of data. In addition to the electronic media, social engineering continues to be a major threat. The ability to impersonate individuals and gain sensitive information is alarming. Education can certainly help to minimize some of the risk.

While the convenience of these consumer technologies has proven to be a necessary part of life for executives in today's data-driven and mobile world, sometimes transferred information can simply fall into the wrong hands. Sensitive data transferred via messages can end up on multiple, unsecured servers where it can be accessed by those who should not be reading it. Intentions may not be malicious, but the end result often is, and that is why survey respondents see a need to invest in encrypting these devices in the year ahead.

It is important to note that in healthcare, more than just the security of data is at stake. Many devices that affect patients' lives can be compromised as well. Medical devices, such as blood pumps, heart monitors and insulin pumps, as well as CT scanners, MRIs and decision support systems warrant the same level of diligent monitoring.

A firewall or anti-virus application is simply not enough of a defense. To adequately safeguard systems, the healthcare provider needs to recognize where it's most vulnerable. If a healthcare organization has not yet identified its weaknesses, then it must be proactive and conduct an information security risk assessment to

uncover potential vulnerabilities and exposures. The assessment will help determine how well critical systems are protected by providing a detailed and full analysis of external and internal threats. In fact, assessments should take place frequently to ensure systems are protected and deployed strategies are proving to be effective.

Finally, it is up to each organization to define and implement

> "A firewall or anti-virus application is simply not enough of a defense."

appropriate processes and procedures that will best narrow the window of exposure. Detection and response are the most critical components of these security measures. Respondents to the survey indicated that the number one technology investment in the upcoming year is audit logs and management. However, these can be of limited value if the numerous events (logs) are not monitored and managed effectively. Due to compliance issues, the complexity of information and the lack of employees with the highly technical skills required to identify these threats, many healthcare organizations are turning to companies like Diebold for help. Teaming with a company like Diebold allows healthcare organizations to tap into around-the-clock monitoring services managed by certified security analysts; gain access to established, well-defined management processes; and obtain a direct connection with subject matter experts that have extensive experience and knowledge of the current threat environment.

Conclusion:
The impacts of a security breach extend far beyond those individual patients that are directly affected. Patients place high importance on privacy and security, and a breach can have immeasurable negative consequences for a healthcare organization's brand reputation as well as its bottom line. Currently healthcare is second only to financial institutions when it comes to breaches, and it's on the rise. As federal regulations and state legislation continue to create complexities, and civil suits relative to breaches become more prevalent, protecting information can no longer take a back seat. Healthcare organizations must make information security a priority; they simply can't afford not to.

About David Kennedy:
David Kennedy is the Chief Security Officer (CSO) for Diebold Incorporated and has a team dedicated to protecting Diebold's infrastructure across 77 countries. Kennedy's team consists of information security, loss prevention, customer compliance, electronic discovery and physical security.

About Diebold Incorporated:
World renowned in the financial market, Diebold Incorporated is also an essential partner in healthcare. Our self-service, service and security solutions protect patient privacy; help ensure the safety of healthcare facilities and their assets as well as simplify transactions for improved efficiency and patient satisfaction. Diebold employs more than 16,000 associates with representation in nearly 90 countries worldwide and is headquartered in the Canton, Ohio region, USA. Diebold is publicly traded on the New York Stock Exchange under the symbol 'DBD.' For more information, visit the company's website. http://www.diebold.com

Other Resources

News
Diebold Earns Online Trust Leadership Award for Dedication to Information Security

http://news.diebold.com/article_display.cfm?article_id=5135

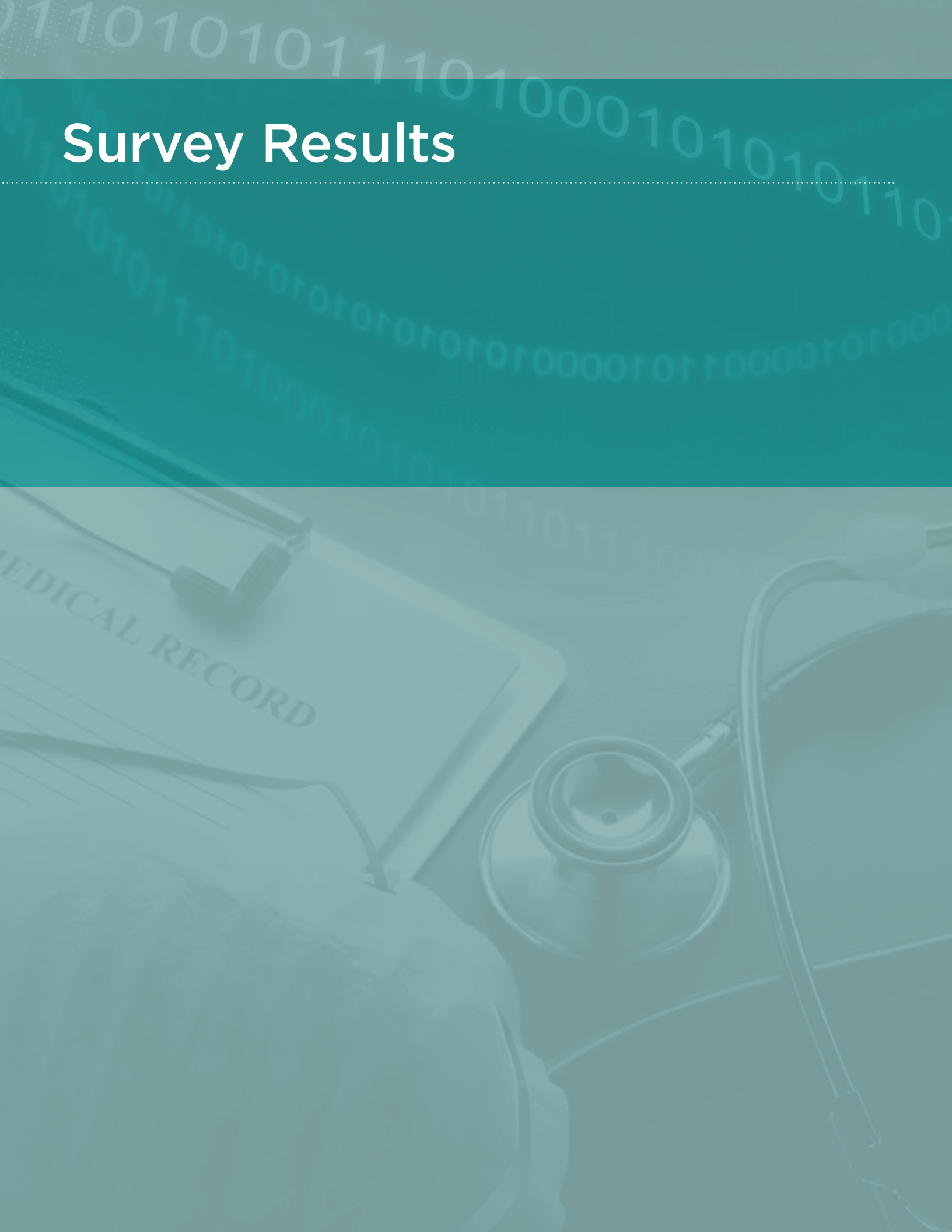
Webinar
Learn realistic insights designed to help healthcare executives leverage healthcare data security that will make a difference – and add value – across the organization.

Managing and Monitoring Healthcare Data - http://bit.ly/rDAIvg

News
Diebold Earns Online Trust Leadership Award for Dedication to Information Security

http://news.diebold.com/article_display.cfm?article_id=5135

Survey Results

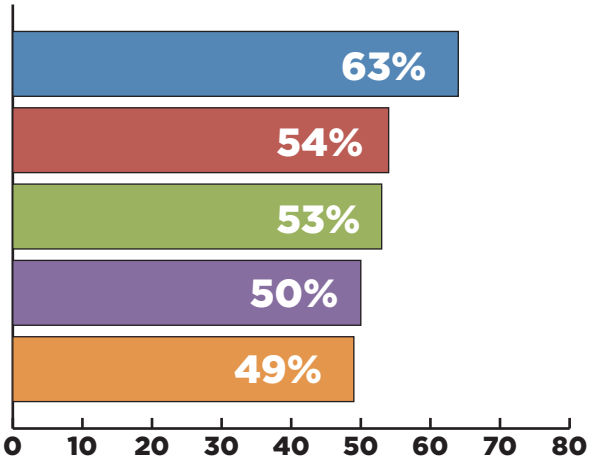


Results

1. Top Priorities. Top Investments.

The inaugural *Healthcare Information Security Today* survey confirms that healthcare organizations still have a lot of work to do, especially in the compliance arena. In fact, improving regulatory compliance efforts ranks as the No. 1 information security priority for the year ahead.

Top Information Security Priorities for Coming Fiscal Year



- 63% - Improving regulatory compliance efforts
- 54% - Improving security awareness/education for physicians, staff, executives and board
- 53% - Improving mobile device security
- 50% - Updating business continuity/disaster recovery plan
- 49% - Preventing/detecting internal breaches

"Executives are seeing large breaches of patient data on front pages, and it is suddenly becoming a much stronger incentive for them to allocate resources to information security," says attorney Adam Greene of the law firm Davis Wright Tremaine (see analysis, page 26). Greene and other experts were given an early look at the survey results so they could offer analysis.

Plus, the Department of Health and Human Services' Office for Civil Rights has ramped up HIPAA enforcement, including fines imposed on such organizations as Massachusetts General Hospital and UCLA Health System for violations. And the office will launch a HIPAA audit program in 2012. "It's becoming increasingly clear that the age of strictly voluntary compliance with respect to HIPAA has come to an end, and the threat of expensive settlements and corrective action plans with federal and state regulators is becoming an increasing reality," says Greene, who formerly was an official at the HHS Office for Civil Rights.

Another compliance catalyst is the federal government's electronic health record incentive program, funded by the HITECH Act, which calls attention to the longstanding HIPAA requirement to conduct a risk assessment. To earn EHR incentive payments, hospitals and clinics must, among many other steps, conduct a risk assessment.

In addition to improving compliance with the HITECH Act, HIPAA and other regulations, a top information security priority for the coming fiscal year is improving security awareness and education for physicians, staff, executives and board members, the survey shows. After all, training plays a key role in breach prevention and regulatory compliance. Another top priority is improving mobile device security, which is not surprising, given the high number of recent major health information breaches involving the loss or theft of such devices.

"I would recommend training be focused on the organization's specific problem areas in addition to overall compliance," Greene says. "So, if there have been laptop thefts, for example, or improper disposal of hard copies or electronic media, make sure the training addresses those issues rather than just doing the same generic training from year to year."

Greene also notes that "the case for encrypting laptops continues to get stronger and stronger." And he adds: "The bigger challenge on mobile devices is probably ... ensuring that protected health information is not left on physician-owned iPads or smart phones."

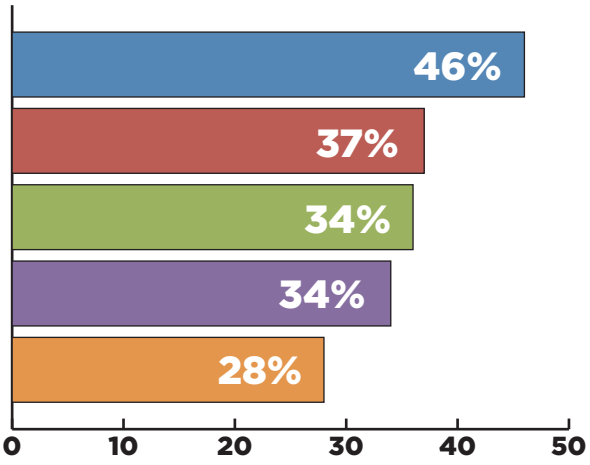
Technologies singled out as top investments for the coming year align closely with top priorities, the survey shows. Heading the list are audit logs and log management, which can help ward off internal threats to avoid HIPAA violations. Other top technology priorities include mobile device encryption, an important breach prevention measure; data loss prevention, which also helps thwart internal breaches; and e-mail encryption, which helps protect against staff mistakenly exposing patient information.

Some experts are surprised that only 25 percent of survey respondents report their organization experienced a breach of any size that had to be reported to the HHS Office for Civil Rights, as required under the HIPAA breach notification rule. Breaches affecting 500 or more individuals must be reported to authorities within 60 days, while smaller breaches must be reported annually. The Office for Civil Rights' tally of major breaches listed more than 340 major incidents as of mid-October. Plus, the office recently informed Congress that more than 30,500 smaller breaches were reported from September 2009 through all of 2010.

"I expect that far more than 25 percent of organizations are experiencing impermissible uses and disclosures of some size, which have the potential to cause reputational or financial harm to individuals," Greene says. "So either organizations' security practices are better than I thought, which is not really suggested by the rest of the survey responses, or organizations may not be looking very hard."

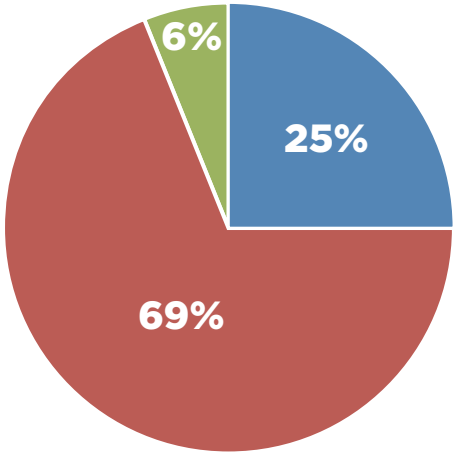
Likewise, Christopher Paidhrin, security compliance officer at PeaceHealth Southwest Medical Center in Vancouver, Wash., believes that the percentage of organizations that have experienced reportable breaches "is much, much higher" than 25 percent.

Top Technology Investments for Coming Fiscal Year



- 46% - Audit logs
- 37% - Mobile device encryption
- 34% - Data loss prevention
- 34% - E-mail encryption
- 28% - Intrusion detection/misuse detection

Has your organization experienced a health information breach of any size that had to be reported to the HHS Office for Civil Rights as required under the breach notification rule?



- 25% - Yes
- 69% - No
- 6% - Don't know

Results

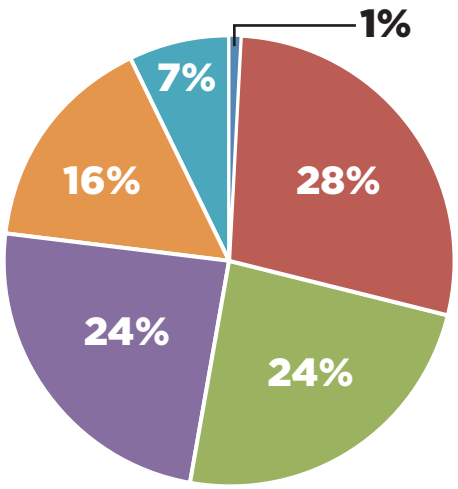
2. Key Threats and Mitigation Steps

Healthcare organizations perceive mistakes by staff members as the single biggest security threat they face. Whether it's leaving a laptop in the back seat of a car or using social media to discuss a patient, staff mistakes can lead to serious security incidents. Insider threats, ranging from inappropriate viewing of records to identity theft, rank second, tied with business associates taking inadequate security precautions for protected health information.

Paidhrin says the perception of staff mistakes and insider threats as top risks should be "a wake-up call for executives to ramp up security training. An unengaged, poorly trained staff will undermine any technology spending or compliance efforts," he says (see analysis, page 29).

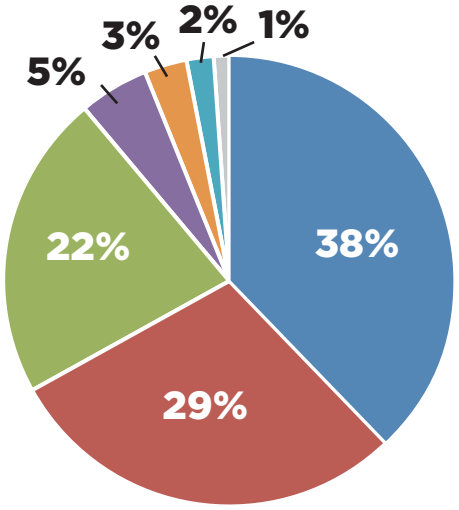
Healthcare organizations still have a long way to go when it comes to countering internal and external threats, the survey shows. Some 43 percent of respondents rank their organization's ability to counter threats as poor, failing or in need of improvement.

What do you perceive to be the single biggest security threat your organization faces?



- 28% - Mistakes by staff members
- 24% - Insider threats, such as records snooping and identity theft
- 24% - Business associates taking inadequate security precautions for protected health information
- 16% - Loss or theft of devices or electronic media
- 7% - Hackers attempting to access records or use servers for other purposes, such as gaming
- 1% - Loss or theft of paper records

How would you grade your organization's ability to counter external and internal information security threats?



- 38% - Needs improvement
- 29% - Adequate
- 22% - Very good
- 5% - Excellent
- 3% - Poor
- 2% - Failing
- 1% - Don't know

"The industry has been weak on keeping up with risk assessments, and by not adequately doing those, they probably haven't really accounted properly for the insider threats," says Terrell Herzig, information security officer at UAB Health System. The Birmingham, Ala.-based integrated delivery system includes a 1,000-bed hospital and numerous clinics.

"Also, clinical staff members have a lot of access rights [for patient information], and the only way to really discover when those access rights have been abused is to examine log files. In looking through the survey, you can tell that a lot of the organizations aren't managing those or looking at those adequately. So it is going to be hard for most organizations to detect when these particular rights are being misused."

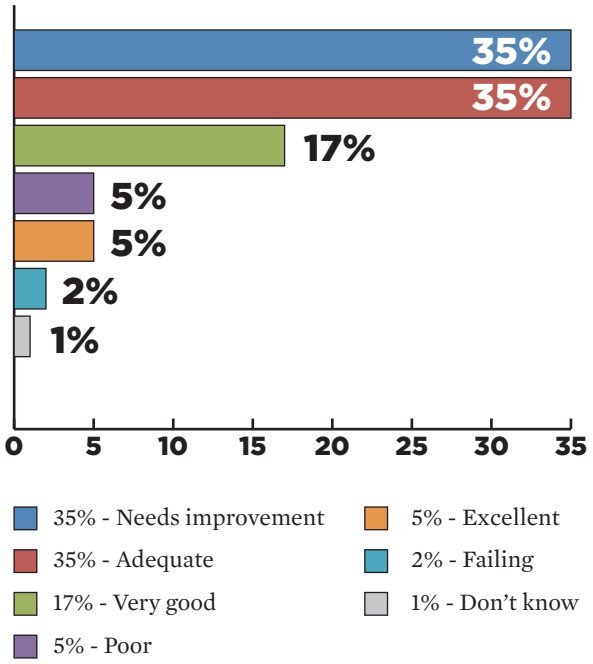
When it comes to external threats, inadequate precautions taken by business associates that have access to patient information is a growing concern. More than 20 percent of major breach incidents reported to federal authorities, including several recent high-profile cases, have involved business associates. For example, a breach affecting 4.9 million TRICARE military health program employees stemmed from backup tapes stolen from the car of a business associate's employee.

"Most organizations don't have visibility into their business associate's operations to be able to even determine if they are monitoring things correctly," Herzig says. "What I have found is that even with an enhanced business associate agreement, business associates will often try to negotiate certain points out. So organizations are going to have to become more aggressive with these business associate agreements and ask for evidence ... of a third-party audit."

An important component of any effort to thwart threats is training. Some 42 percent of respondents grade the effectiveness of their security training and awareness activities as poor, failing or in need of improvement.

"A lot of organizations did their initial HIPAA training as required, and that was pretty much the extent of the training they offered," Herzig laments (see analysis, page 19).

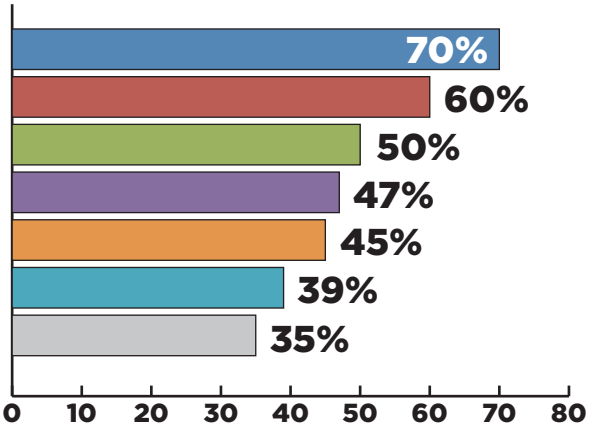
How would you grade the effectiveness of your security training and awareness activities for staff members and physicians?



Another important risk management strategy is the use of encryption. After all, under HIPAA's breach notification rule, breaches don't have to be reported if the data involved is properly encrypted.

Yet the survey finds that only 60 percent of organizations apply encryption to mobile devices. Given the large number of major breaches involving lost or stolen devices, it's not surprising that encrypting these devices ranked as the No. 2 technology investment for the year ahead.

Specify whether your organization currently applies encryption for:



- 70% - Information sent outside the organization across exposed external networks
- 60% - Mobile devices
- 50% - Backup tapes
- 47% - Information accessible via a virtual private network
- 45% - Mobile storage media, including USB drives
- 39% - Desktop PCs
- 35% - Servers/databases

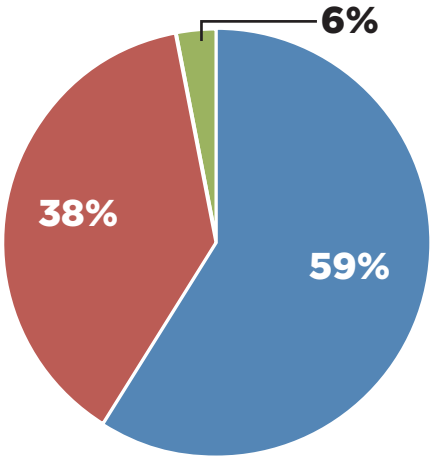
Several recent major breaches, including the TRICARE incident, have involved the loss or theft of unencrypted backup tapes. The survey illustrates the level of risk that still exists: Only half of organizations encrypt backup tapes.

The movement to mobile devices brings new risks. The survey shows that 59 percent of organizations allow physicians and other clinicians to use personal devices for work-related purposes. Some 70 percent of respondents have a mobile device security policy in place.

Of those that have a mobile device security policy, key components include requiring all portable media to be encrypted and requiring patient data stored on or transmitted from mobile devices to be encrypted, the survey shows. More than half of those with a mobile device security policy say they prohibit storage of data on mobile devices to minimize risk.

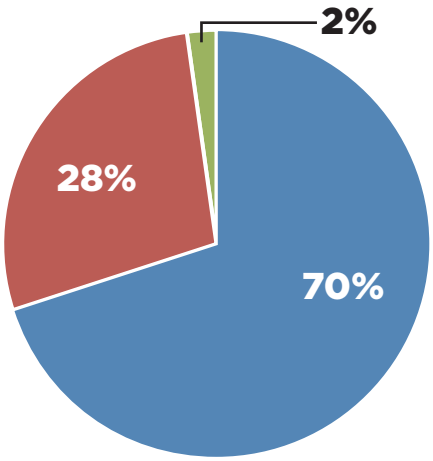
"Before any decisions are made regarding a mobile device, you really need to assess how a device is going to be used and what threat it is going to pose to the organization," Herzig stresses. Healthcare organizations need to determine whether to restrict mobile devices used to access clinical data to those that are corporate-owned or to also allow the use of personally owned devices "that meet certain technical controls and policy basics," Herzig says. Staff training on mobile device security is essential, he notes.

Does your organization allow physicians and/or other clinicians to use their personal mobile devices for work-related purposes?



59% - Yes 38% - No 6% - Don't know

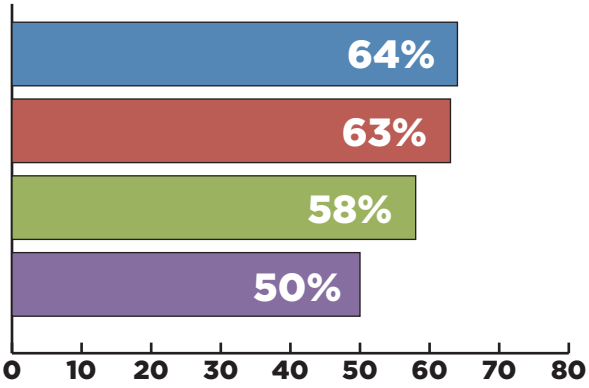
Does your organization have a mobile device security policy?



70% - Yes 28% - No 2% - Don't know

The survey shows 80 percent of organizations offer physicians remote access to clinical systems. For those that do, security is most commonly addressed by providing access only via a virtual private network.

What are the major components of your mobile device security policy?



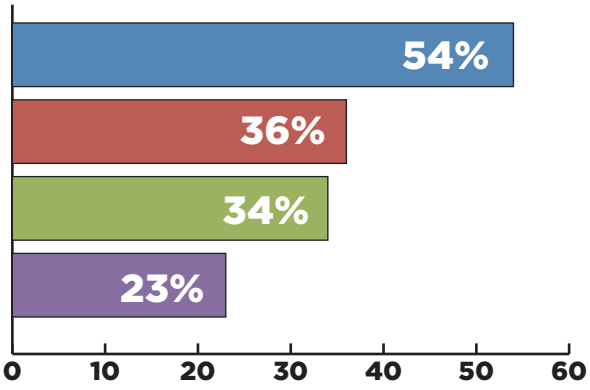
- 64% - All portable media must be encrypted
- 63% - Patient data stored or transmitted from all mobile devices must be encrypted
- 58% - Prohibit storage of data on mobile devices
- 50% - All staff must take education session on the policy

High-profile incidents involving inappropriate posting of patient information on social media sites have called attention to the need to educate staff about the use of Twitter, Facebook and other options. Yet only 54 percent of responding organizations have a formal security policy in place governing the use of social media. Of those that do, 63 percent have imposed disciplinary action against an employee for violating the policy.

Some 52 percent of organizations are participating in a health information exchange. Of those, 56 percent send health information to be stored in a separate repository operated by the HIE organization, while 44 percent allow the HIE organization to query and pull information from the organization's information systems, using what's called a federated model.

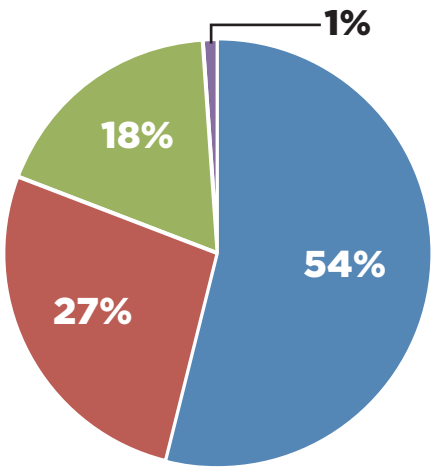
Some advocates of the federated model, including organizers of a statewide HIE-Bridge in Minnesota, argue that it helps assure privacy by giving participating organizations more control over sensitive data.

How do you address security for remote access?



- 54% - Provide access to clinical systems only via a virtual private network
- 36% - Require physicians to use multifactor authentication
- 34% - Encrypt all information accessed remotely
- 23% - For access via personal mobile devices, require use of specific devices

Does your organization have a formal security policy governing the use of social media?



- 54% - Yes
- 27% - No
- 18% - In development
- 1% - Don't know

Staff Training: Effective Techniques

Terrell Herzig, Information Security Officer, UAB Health

HEALTHCAREINFOSECURITY: Why aren't more organizations making solid progress on information security training?

TERRELL HERZIG: A lot of organizations did their initial HIPAA training as required and that was pretty much the extent of the training they offered. ... What I have found is that there are two fronts you need to train people on. Certainly, they need to know your organization's policies and procedures as they pertain to protected health information, but you also need to be able to train those individuals effectively on technology. They need to understand why it's not a good idea to bring in cell phone "x" that is the new tool out on the market but that may, indeed, be exposing the organization to potential data loss. ...

It's not necessary to have a lot of town hall meetings to educate folks, because clinical staffs are very busy. ... Here we use newsletters; we use e-mail. ... I'll come in, for example, on a Monday morning and send out a mass mailing [noting] some ... security events that we're seeing [in the news] and people like reading those because it tells them things that they were not familiar with. [We also offer] brown bag lunches where we talk about a certain topic, like ... how to harden your PC against threats like malware.

HEALTHCAREINFOSECURITY: Only 46 percent of those surveyed say they update their business continuity planning annually. Why is it essential to frequently update a business continuity plan based on your experience? I know you just went through the tornado there in Alabama.

HERZIG: You never know what Mother Nature may throw at you and what size or magnitude of a natural disaster you may find yourself exposed to, so it is very important that you review those disaster recovery plans and make sure that ... you are ready to deal with a community-wide disaster when it occurs.

Part of that, too, is an ongoing measurement to make sure that your contingency plans and your critical systems have been routinely inspected and evaluated to make sure that any impact to those systems can be recovered on a timely basis.

Terell Herzig

"A lot of organizations did their internal HIPAA training and that was pretty much the extent of the training that they offered."

... Business impact assessments ... should be reevaluated at least on an annual basis so that senior management will have an understanding of how long it would take to recover service if it went down, or if there is a need to go out and invest in technologies with faster response times. ...

Listen to the interview:
http://www.healthcareinfosecurity.com/podcasts.php?podcastID=1271

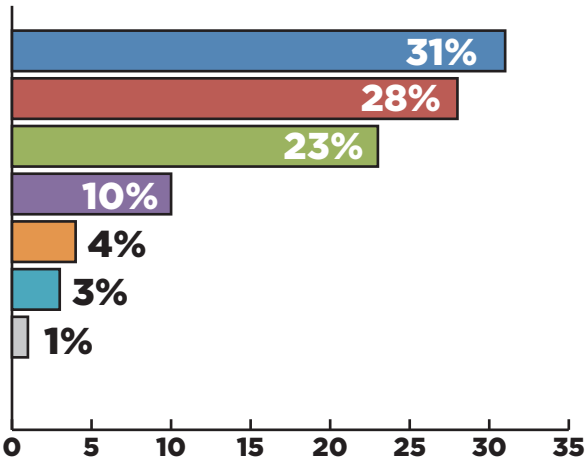
Results

3. Compliance: Keeping Up is a Challenge

As noted earlier, improving regulatory compliance is the No. 1 security priority for the year ahead. That includes compliance with the HIPAA privacy and security rules, the HITECH mandated HIPAA breach notification rule and more. Asked to grade their organization's ability to comply with HIPAA and HITECH Act regulations on privacy and security, survey participants assign widely varying ratings (see chart).

The HIPAA Security rule, in effect since 2005, requires organizations to conduct a risk assessment. Yet the survey shows that 26% of organizations have yet to conduct one. Of those that have conducted a risk assessment, 63 percent did it with the help of a third party.

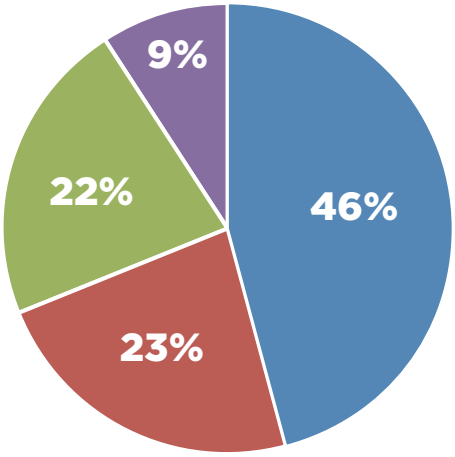
How would you grade your organization's ability to comply with HIPAA and HITECH Act regulations concerning privacy and security?



- 31% - Adequate
- 28% - Very good
- 23% - Needs improvement
- 10% - Excellent
- 4% - Poor
- 3% - Failing
- 1% - Don't know

About 46 percent of organizations with risk assessments update them annually.

How often do you update your risk assessment?

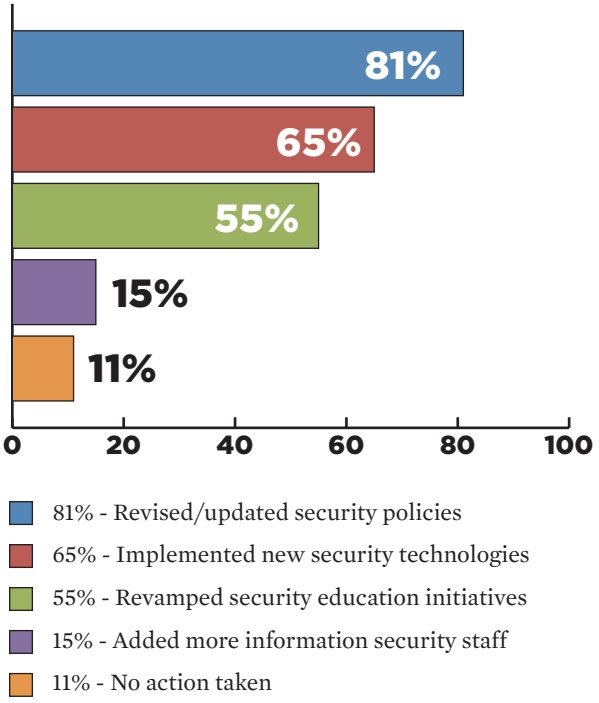


- 46% - At least annually
- 23% - Every two-three years
- 22% - No set time period
- 9% - Whenever there is a major change, such as a new application is installed

The most common actions taken as a result of a risk assessment are revising and updating security policies and implementing new security technologies.

"In a world of exceedingly limited resources, risk assessments have a hard time rising to the top of the budget list," Greene says. "Smaller organizations may not even know where to start, or may not have placed HIPAA security rule compliance as a big priority. Large organizations may view it as a large, expensive effort that will only lead to more expenses as threats and vulnerabilities are highlighted, especially if the possibility of enforcement is remote."

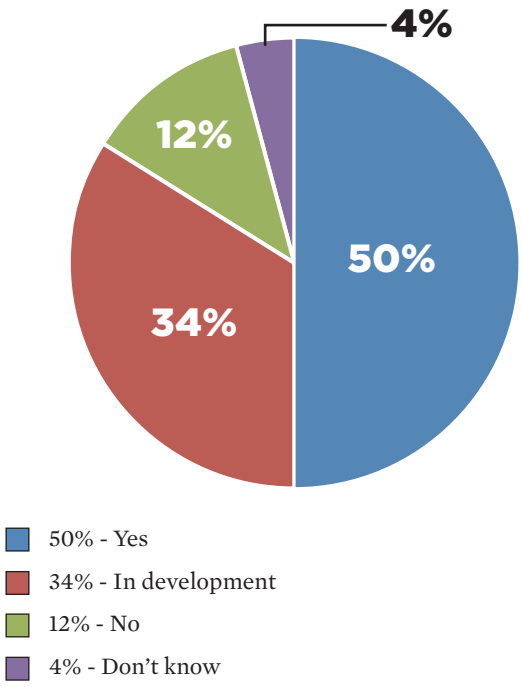
What action have you taken as a result of your risk assessment?



But Greene believes organizations lacking risk assessments will be forced to get up to speed as HIPAA compliance enforcement ramps up. And he stresses that risk assessments should be updated annually. "There are no hard and fast rules, but the state of technology and the threats out there change so rapidly that doing, for example, a risk assessment every three years is probably not going to cut it in the eyes of regulators," he says.

The HIPAA interim final breach notification rule, mandated by the HITECH Act, has been in effect since September 2009. Yet only half of survey respondents have a detailed plan in place to comply with the rule. Of organizations that have a plan in place, less than half have tested it.

Does your organization have a detailed plan in place to comply with the HITECH Act's breach notification rule?



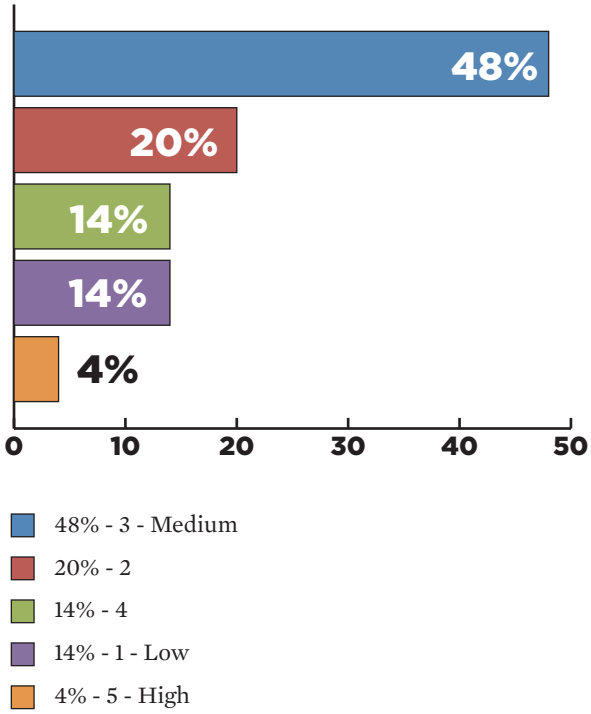
"Some organizations may think that they will simply deal with breaches as they arise, and that either they do not need to, or do not want to, proactively seek to detect breaches," Greene says. "If an organization does not have a breach [detection and notification] plan, it will not proactively find breaches, and this is rolling the dice with a potential for hundreds of thousands or millions of dollars in penalties."

Greene recommends that organizations assign information security staff to "proactively audit records to find potential breaches. There are various ways to do auditing, but it is important to do smart auditing rather than just a completely random sample. There are certainly tools available to do algorithms that may hone in on potential problem areas."

The attorney and former HIPAA enforcer also urges organizations to "ensure that all staff are trained to recognize what is protected health information, because sometimes this is not fully understood, and [ensure that they understand] when PHI may have been breached and to whom to report a breach."

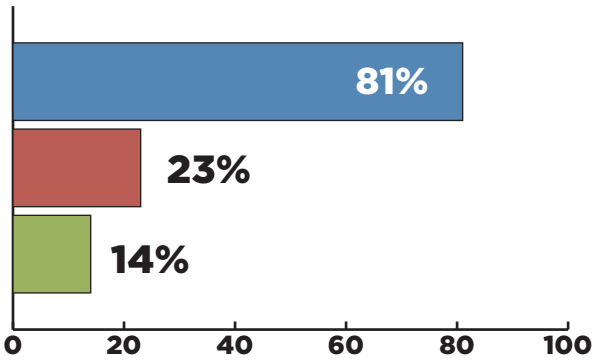
Asked to rate their confidence in the security controls maintained by business associates and their subcontractors, only 18 percent give them high marks (see chart).

On a scale of 1-5, how would you rate your confidence in the security controls maintained by your business associates and their subcontractors?



To make sure that business associates are complying with HITECH and HIPAA, most organizations have modified business associate agreements to add more details. While many experts advise healthcare organizations to ask business associates for a copy of their security policy, as well as the results of a third-party security audit, relatively few organizations have taken those steps, the survey shows.

What steps have you taken to ensure that your business associates that have access to protected health information are HITECH Act and HIPAA compliant?

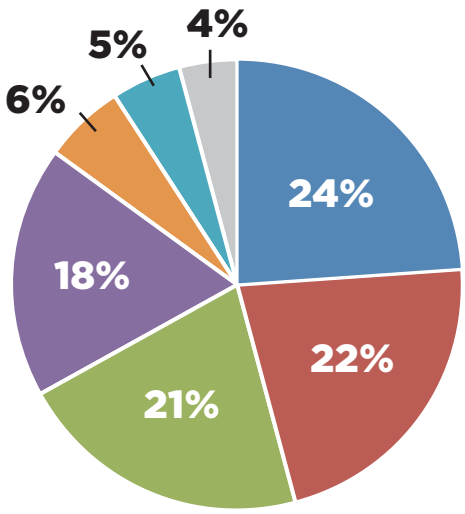


- 81% - Modified business associate agreement to provide more details
- 23% - Obtained a copy of BA's security policy
- 14% - Obtained a copy of BA's security audit

A business associate agreement should include details about how quickly the vendor needs to report a breach, says Herzig of UAB Health System. "You certainly don't want the business associate taking 50 days to investigate a situation and notify you, and then you've only got a short time to conduct your investigation and notify patients."

Regarding their ability to comply with the Payment Card Industry Data Security Standard, 27 percent grade their organization as poor, failing or in need of improvement.

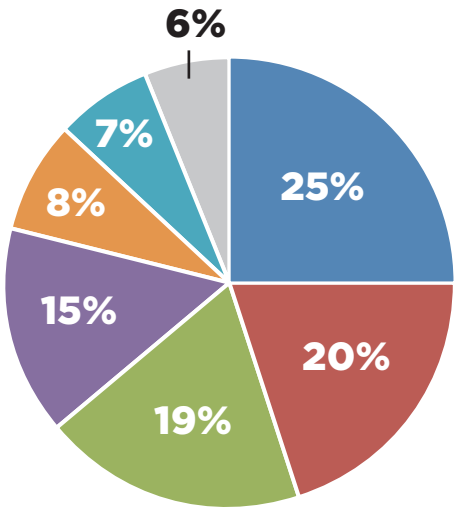
How would you grade your organization's ability to comply with the Payment Card Industry Data Security Standard, or PCI DSS?



- 24% - Adequate
- 6% - Excellent
- 22% - Very good
- 5% - Poor
- 21% - Don't Know
- 4% - Failing
- 18% - Needs improvement

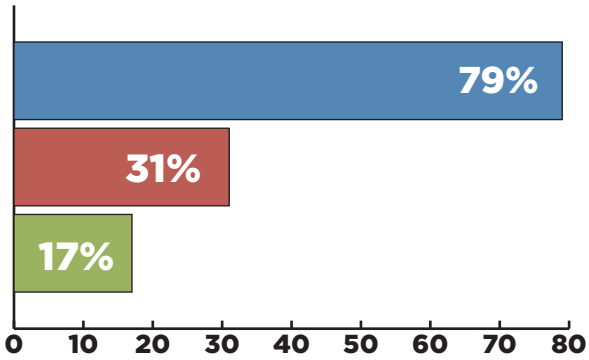
A proposed Accounting of Disclosures Rule would require providing patients, upon request, with an access report listing everyone who has viewed their "designated record set." A majority of respondents say they would grade their organization's ability to meet the requirements of the proposed rule as poor, failing or in need of improvement. The biggest area of concern is that their applications lack audit functionality or they have inadequate capabilities to aggregate log data from multiple systems.

How would you grade your organization's ability to meet the requirements in the proposed Accounting of Disclosures Rule, including providing patients, upon request, with an access report listing everyone who has viewed their "designated record set?"



- 25% - Needs improvement
- 8% - Don't Know
- 20% - Adequate
- 7% - Failing
- 19% - Poor
- 6% - Excellent
- 15% - Very good

How does your organization track who accesses protected health information?

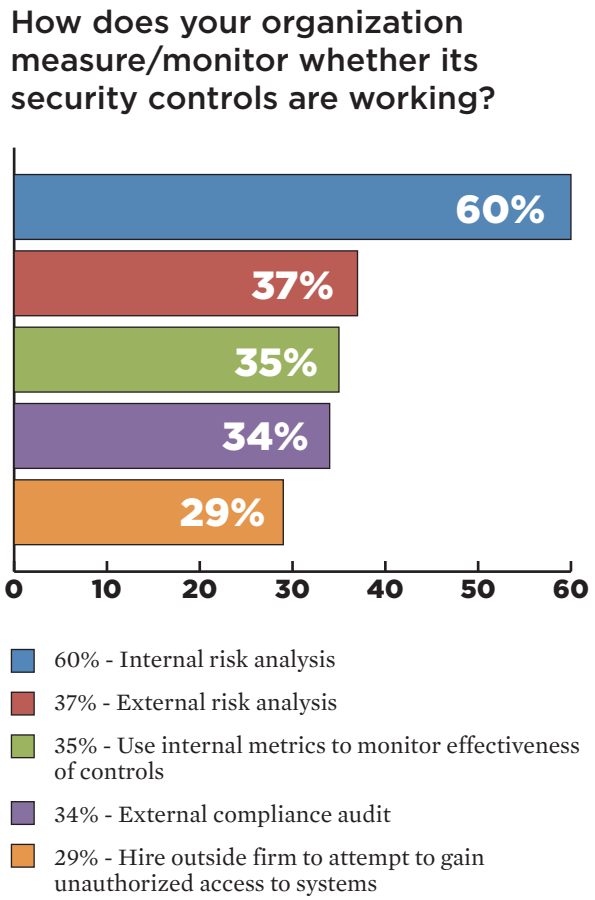


- 79% - Use audit functions within our applications
- 31% - Use a separate audit log application
- 17% - Use a data loss prevention application

Tracking who accesses protected health information would be an important component of compliance with the Accounting of Disclosures Rule. It also plays a vital role in monitoring against various insider threats. The survey finds that the most common method for tracking access, by far, is by using audit functions within applications, rather than using a separate audit log or data loss prevention application.

The most common method organizations use to measure whether their security controls are working is through an internal risk analysis. Herzig called this one of the biggest surprises in the survey.

"Risk assessments traditionally tell you where your risks are, and the likelihood for them having an impact," he says. Instead, organizations should create specific metrics for measuring the effectiveness of security controls, Herzig contends.



Analysis

Will Security Become a Budget Priority Item?

Adam Greene, Partner, Davis Wright Tremaine (formerly an HHS official)

HEALTHCAREINFOSECURITY: Why do you think that information security is not yet a higher priority for many?

ADAM GREENE: Information security has been a victim of budget triage. Every organization would like to have robust security but probably feels the need to place their resources elsewhere. This may be due to a lack of enforcement and transparency in the past. Only a few years ago, if you had a security incident, it was unlikely to attract the attention of regulators or patients, and it was therefore unlikely to result in enforcement problems or reputational damage. So the incentives were not necessarily there to put much of your resources into security. This really began to change with state breach notification laws, when organizations suddenly had to start airing their dirty laundry with respect to security incidents. This resulted in significant hits to reputations, and that led to an increase in security as a priority. And that is going to increase even more as state and federal enforcement picks up in this area.

HEALTHCAREINFOSECURITY: The survey finds that improving regulatory compliance efforts was the number one information security priority for healthcare organizations in the coming year. Why is that the case?

GREENE: ...Executives are seeing large breaches of patient data on front pages, and it is suddenly becoming a much stronger incentive for them to allocate resources to information security. Additionally, it's becoming increasingly clear that the age of strictly voluntary compliance with respect to HIPAA has come to an end, and the threat of expensive settlements and corrective action plans with federal and state regulators is becoming an increasing reality. Finally, I wouldn't underestimate the impact of the meaningful use [HITECH Act electronic health record incentive] program, and the requirement to attest to a risk analysis and risk management program. For many, this is really the first time that they are vouching for their organization's security.

HEALTHCAREINFOSECURITY: Speaking of risk assessments, the survey shows that about a quarter of organizations have yet to conduct one, even though such an assessment has been required


Adam Greene

under HIPAA for a number of years. Why are so many still lagging?

GREENE: In a world of exceedingly limited resources, risk assessments have a hard time rising to the top of the budget list. ... The percentage of [organizations that have a current] risk assessment will increase as enforcement increases. For example, based on these survey numbers, it appears inevitable that a significant portion of the upcoming 150 [HIPAA compliance] audits will find covered entities with no risk assessment, and those may be some of the most likely candidates for referral to the Office for Civil Rights investigators and for the possibility of formal enforcement.

Listen to the interview:
http://www.healthcareinfosecurity.com/podcasts.php?podcastID=1269

Results

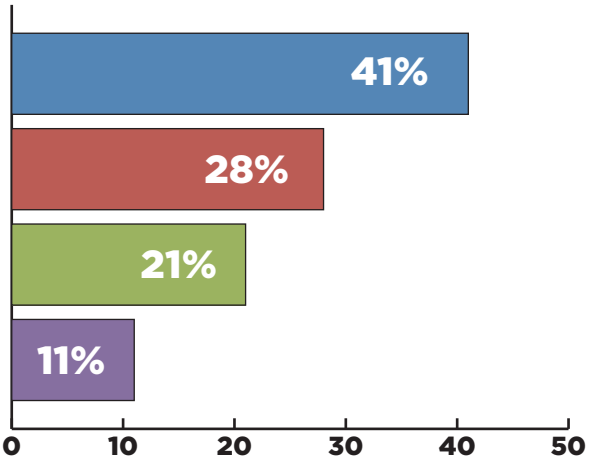
4. Resources: Staffing and Budgeting Woes

Despite all the headlines about healthcare information breaches and public concerns about privacy, the survey confirms that winning financial support for security efforts continues to be a challenge.

Only 60 percent of organizations have a documented information security strategy in place, while 28 percent say they are "working on it," and 12 percent lack a strategy.

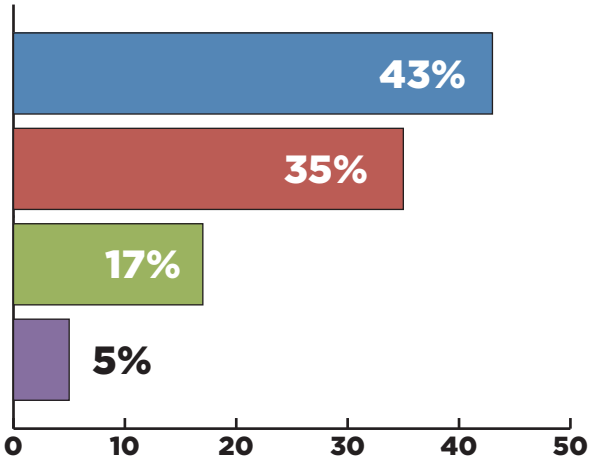
Some 69 percent of those surveyed estimate that their organization devotes 3 percent or less of its IT budget to information security. But 43 percent expect that percentage to increase in the coming fiscal year.

What percentage of your total IT budget for the current fiscal year is devoted to information security?



- 41% - 1 to 3 percent
- 28% - Less than 1 percent
- 21% - 4 to 6 percent
- 11% - 7 percent or more

How do you expect that percentage to change in the next fiscal year?

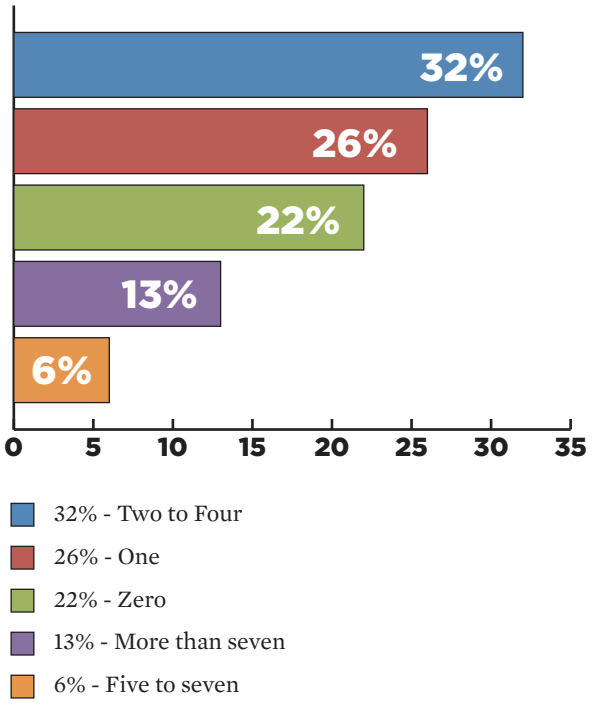


- 43% - Increase
- 35% - Stay the same
- 17% - Don't know
- 5% - Decrease

A large majority - 65 percent - say they do not have a portion of their IT budget specifically allocated for breach detection, response and notification costs.

Some 22 percent of organizations report that they have no full-time staff members who devote most or all of their time to information security. A substantial majority – 58 percent - say they have one to four staff members devoted to security.

How many full-time staff members in your organization devote most or all of their time to information security?



Chief information security officers are in place at 59 percent of organizations surveyed. And only 43 percent report having a defined information security budget.

"Money is tight. Healthcare executives are challenged by the loss of revenue, especially with ever-lowering reimbursement rates, and the overall cost of healthcare is increasing, but little of it benefits the provider," says Paidhrin of Southwest Medical Center.

"So IT security is considered a luxury that few can afford. ... It's a technology cost center. And the top priorities are making payroll and reducing the reimbursement cycle. Security is largely seen as a necessity, like a cleaning service ... but it is not a top priority."

But Paidhrin isn't surprised by the expectation that IT security budgets will increase.

"As healthcare leaders discover how much more vulnerable their information systems are, and the real costs for breaches, the return on investment calculus is shifting," he says. As more clinicians and other staff members use mobile devices, "that alone will greatly increase vulnerability concerns and costs," he notes.

Analysis

Winning Support for Security Spending

Christopher Paidhrin, Security Compliance Officer, PeaceHealth Southwest Medical Center

HEALTHCAREINFOSECURITY: About 70 percent of organizations estimate that they devote 3 percent or less of their IT budget to information security. But 43 percent expect that percentage to increase in the coming year. What's the best way to determine an adequate level of spending for security?

CHRISTOPHER PAIDHRIN: IT infrastructure and the skilled people to make it work are expensive, often 80 percent or 90 percent of IT budgets. IT security is most often a part-time or single-person role, and there may be a batch of policies, and, if the organization is fortunate, a small handful of technologies - usually the minimum necessary - to get the essential job done, namely, protecting information.

I'm not surprised by the expectation that IT security budget funding will increase. As healthcare leaders discover how much more vulnerable their information systems are, and the real costs for breaches, the return on investment calculus is shifting. Examples are the explosion of tablet use and "bring-your-own" devices. Providers and staff want mobile connectivity, and that alone will greatly increase vulnerability concerns and costs.

HEALTHCAREINFOSECURITY: Based on your experience, what is the key to winning senior executive support for staffing and funding for information security?

PAIDHRIN: ...Winning executive support takes both skill and a strong argument, and a solid business case set of justifications. The key is to focus a business case for security in no more than four bullet-point slides. Each organizational priority must have a directly associated security tag that shows why security strengthens and aligns with each priority. Executives want to do the right thing; they just need a clear reason to do it.

HEALTHCAREINFOSECURITY: Top information security technology investments for the coming year, according to this survey, are audit logs, mobile device encryption, data loss prevention, and e-mail encryption. Why do you think those are the priorities?

Christopher Paidhrin

"Winning executive support takes a solid business case."

PAIDHRIN: ... The more mobile the workforce becomes, the more healthcare becomes outpatient-centric ... the greater the risks. Each of these technologies addresses an aspect of information on the move. Audit logs are a HIPAA requirement, but mobile device and e-mail encryption address information in transit, and data loss prevention is another layer of information and risk containment. It is all about extending security controls to where the information is located. ...

Listen to the interview:
http://www.healthcareinfosecurity.com/podcasts.php?podcastID=1270

Results

5. Cloud Computing: Untested Waters

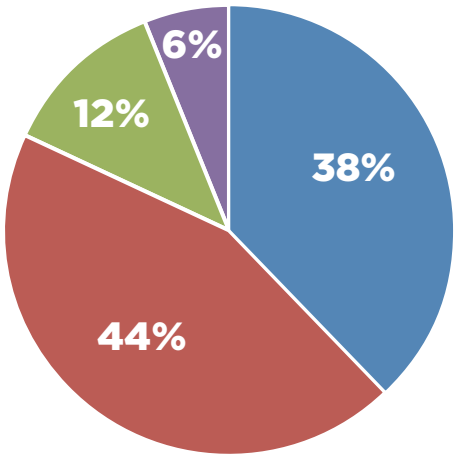
Only 38 percent of those surveyed report that their organization is using cloud computing for such purposes as remotely hosting applications or for storing data and images. Among those not using cloud computing, the biggest reservation cited is enforcing security policies and HIPAA compliance.

Of those that are using cloud computing, 54 percent say they are somewhat confident in the vendor's security policies and procedures, while 28 percent are very confident and 18 percent are not confident.

Before negotiating a contract with a cloud computing vendor, organizations should ask plenty of questions about privacy and security, says consultant Chris Witt of Wake Technology Services.

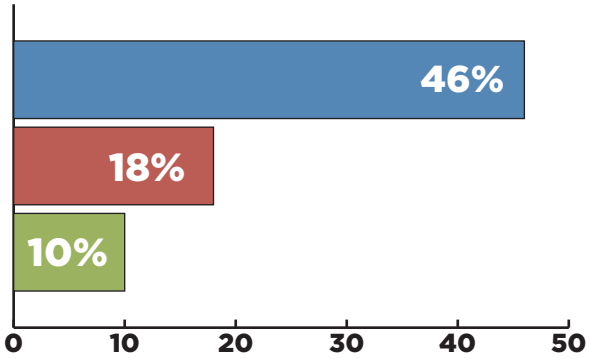
"If you're not comfortable with how the cloud vendor runs their operation, and you're not 100 percent confident that they can provide similar or even better protections than you are already providing, then you probably should not be moving forward with that vendor," Witt says.

Does your organization use cloud computing, such as for remotely hosting applications or for data/image storage?



- 38% - Yes
- 44% - No
- 12% - In development
- 6% - Don't know

If your organization is not using cloud computing, what is your biggest reservation?



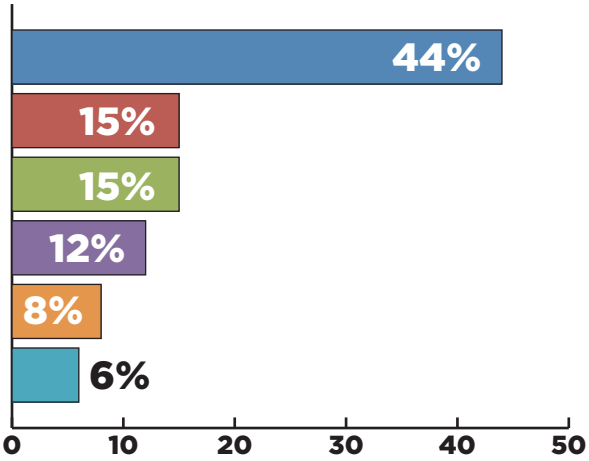
- 46% - Enforcing security policy and HIPAA compliance
- 18% - Data loss prevention
- 10% - Cost

Results

6. Business Continuity: A Status Report

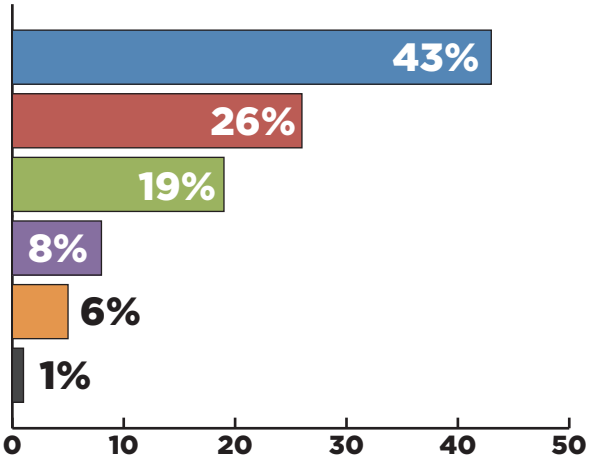
The survey shows that about 94 percent of organizations have a business continuity plan in place to help ensure the availability and security of information in the event of a disaster. Only 20 percent have ever had to activate their business continuity plan. And less than half update and test their plan annually.

How often do you update your business continuity/contingency plan?



- 44% - Annually
- 15% - Every two years
- 15% - No set time period
- 12% - No update in last 3 years
- 8% - Every three years
- 6% - We do not have a plan

How often do you test your business continuity/contingency plan?



- 43% - Annually
- 26% - No set time period
- 19% - We have not tested our plan
- 8% - Every two years
- 6% - We do not have a plan
- 1% - Every three years

Organizations use a variety of methods to test their business continuity plans. The most common are desktop exercises and actual fail-over of equipment and systems. Annual updates of business continuity plans are essential, says Herzig of UAB Health System, which dealt with the impact of a tornado early in 2011.

"You never know what Mother Nature may throw at you and what size or magnitude of a natural disaster you may find yourself exposed to," he says. "So it is very important that you review those disaster recovery plans and make sure that ... you are ready to deal with a community-wide disaster."

The Agenda

When it comes to information security, healthcare organizations still have a lot of work to do, the survey confirms. Here are some action items for 2012:

Conduct, Update Risk Assessments

The one-fourth of organizations that lack a risk assessment will need to get up to speed to help prevent breaches and comply with HIPAA and the HITECH Act. With HIPAA compliance audits looming, the lack of a risk assessment could potentially result in serious penalties. And many organizations are long-overdue for a risk assessment update.

Prepare for Breach Notification

A top priority for many organizations will be developing a detailed plan to comply with the HITECH Act's breach notification rule. The survey shows half lack such a plan that outlines a strategy for both preventing and detecting breaches, as well as to promptly notify those affected by security incidents. And once the final version of the HIPAA breach notification rule is released, all organizations will need to review their compliance efforts to make sure they meet the very latest requirements.

Closely Monitor Business Associates

Because so many of the larger health information breaches have involved business associates, more healthcare organizations will be more carefully scrutinizing their vendor partners. "So organizations are going to have to become more aggressive with these business associate agreements ... and ask for proof they've been audited by a third party," says UAB Health System's Herzig.

Protect Electronic Health Records

As more hospitals and clinics adopt electronic health records and apply for HITECH incentives, they'll need to take steps to ensure the newly digitized information is secure. That includes taking advantage of such technologies as encryption and user authentication. Plus, as more organizations participate in health information exchanges, they'll be scrutinizing the security policies and procedures in place to protect data that's exchanged.

Invest in New Technologies

The survey shows healthcare organizations will be investing in audit logs, mobile device encryption, data loss prevention, e-mail encryption and intrusion detection, among other technologies, to help prevent breaches. "It's all about extending security controls to where the information is located," says Paidhrin of Southwest Medical Center.

Create Bigger Security Budgets

After years of low spending on information security, more organizations are planning to ramp up their security budgets, recognizing that as more information is digitized, more protections are needed.

Boost Business Continuity Planning

Because less than half of organizations update their business continuity plans annually, a majority have out-of-date plans that may fail to meet their needs in an emergency. In the wake of tornadoes, hurricanes and other natural disasters in 2011, look for more organizations to scrutinize and update their disaster recovery and business continuity plans.

Resources

Learn more about key healthcare information security issues:

The New HIPAA Enforcer

Leon Rodriguez, the new director of the HHS Office for Civil Rights, outlines his HIPAA enforcement priorities and his plans for educating healthcare organizations about compliance.

http://www.healthcareinfosecurity.com/podcasts.php?podcastID=1258

Questions to Ask Cloud Vendors

Security consultant Chris Witt offers practical advice on sizing up cloud computing vendors, including a list of essential privacy and security questions to pose.

http://www.healthcareinfosecurity.com/podcasts.php?podcastID=1210

Breach Notification Planning Tips

Security consultant Bob Chaput describes the requirements of the HIPAA breach notification rule and outlines key compliance steps.

http://www.healthcareinfosecurity.com/podcasts.php?podcastID=1113

Managing Business Associates: Practical Guidance

In this webinar, security consultant Kate Borten offers insights on how to work with business associates to prevent health information breaches.

http://www.healthcareinfosecurity.com/webinarsDetails.php?webinarID=235

Business Continuity for Hospitals

In this webinar, Terrell Herzig of UAB Health System, whose organization coped with tornadoes that ravaged Alabama, outlines how to create an effective business continuity plan.

http://www.healthcareinfosecurity.com/webinarsDetails.php?webinarID=234

About ISMG

Headquartered in Princeton, New Jersey, Information Security Media Group, Corp. (ISMG) is a media company focusing on Information Technology Risk Management for vertical industries. The company provides news, training, education and other related content for risk management professionals in their respective industries.

This information is used by ISMG's subscribers in a variety of ways—researching for a specific information security compliance issue, learning from their peers in the industry, gaining insights into compliance-related regulatory guidance and simply keeping up with the Information Technology Risk Management landscape.

Contact

ISMG Sales Team
(800) 944-0401
sales@ismgcorp.com

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification.

ISMG INFORMATION SECURITY MEDIA GROUP

4 Independence Way • Princeton, NJ • 08540 • www.ismgcorp.com