SURVEY RESULTS
REPORT

HEALTHCARE INFORMATION SECURITY TODAY

2013 Outlook: Survey Offers Update on Safeguarding Patient Information

INSIDE

Complete Survey Results

In-Depth Analysis

Expert Commentary

iSMG
INFORMATION SECURITY
MEDIA GROUP

From the Editor

Health Info Security: Work to be Done

Survey Offers Reality Check on Safeguarding Patient Information

Howard Anderson
News Editor, ISMG

Electronic health records are becoming more pervasive at hospitals and clinics alike as HITECH Act incentive payments continue. Meanwhile, healthcare organizations are taking small steps toward meaningful exchange of patient information.

The digital transformation of healthcare holds great promise for dramatically improving the quality of care while holding down costs by providing timely access to potentially live-saving information.

But the January release of the HIPAA Omnibus Rule, with tougher privacy and security requirements and tougher penalties, called attention yet again to the need for healthcare organizations to ramp up their efforts to safeguard patient information.

The more than 570 major breach incidents added to the federal tally since September 2009 also offer a grim reminder that there, indeed, is plenty of security work yet to be done.

So what steps are hospitals, clinics, insurers and others taking this year to help prevent breaches and boost security? The second annual Healthcare Information Security Today survey provides answers.

This handbook offers an in-depth look at the strengths and weaknesses of healthcare organizations' security programs. While it shows many organizations still have a long way to go when it comes to adopting security technologies, such as encryption, it also shows 2013 is a year when many plan to take significant action.

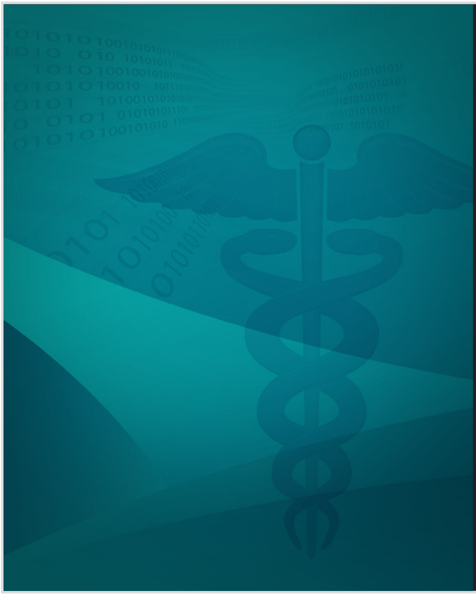
The handbook that follows provides an analysis of the survey results, offering a reality check on the state of healthcare information security.

Howard Anderson
News Editor
Information Security Media Group

Contents

Healthcare Information Security Today

2013 Outlook: Survey Offers Update on Safeguarding Patient Information



Survey Results

Sponsored by RSA

RSA is the Security Division of EMC, a premier provider of security, risk and compliance management solutions for business acceleration. RSA helps organizations solve their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments. www.emc.com/rsa

Introduction: What Is This Survey About?

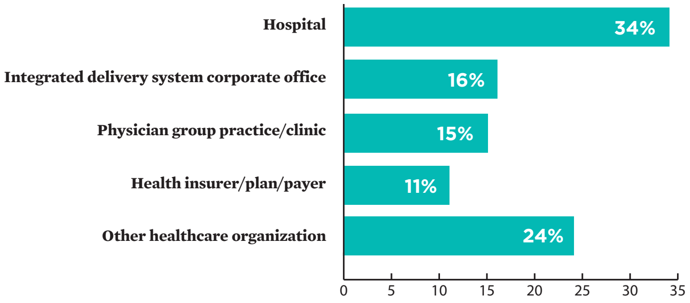
As hospitals, clinics and other healthcare organizations implement electronic health records and participate in health information exchange, they're working to develop robust information security measures to assure patients that their information will be protected – and win their trust.

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

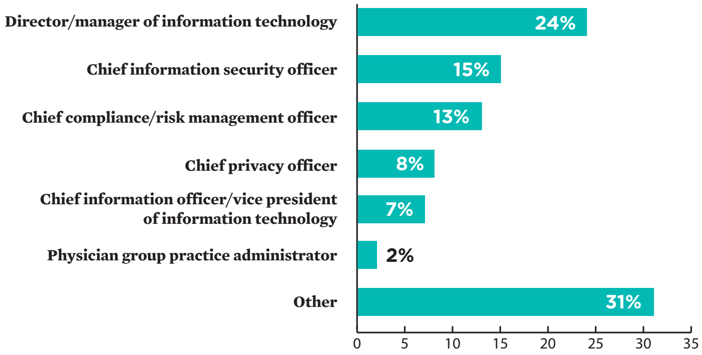
The survey was developed by the editorial staff of Information Security Media Group, with the assistance of members of the *HealthcareInfoSecurity* board of advisers, which includes leading healthcare information security and IT experts. RSA, the Security Division of EMC, supported the survey as sponsor.

The online survey was conducted in the fall of 2012. Respondents included nearly 200 chief information security officers, CIOs, directors of IT and other senior leaders. These executives work at hospitals, integrated delivery systems, physician group practices, insurers and other healthcare organizations.

What type of organization do you work for?



What is your title?



Hot Topics

The new survey helps pinpoint a number of hot topics in healthcare information security

1. Breach Prevention: Emerging Priorities

Healthcare organizations are more confident in their ability to thwart external threats than they are about mitigating internal threats. As a result, the top breach prevention strategy is stepped-up training.

2. Encryption and Authentication: A Long Way to Go

Encryption and authentication can play critical roles in preventing breaches. But the survey confirms that healthcare organizations still have a lot of work to do in implementing these technologies.

3. Risk Assessments: Keeping Up Is a Challenge

HIPAA and the HITECH Act both require current risk assessments. Yet the survey shows about a third of organizations have not conducted an assessment within the past year, which means they may not be addressing evolving risks.

4. Top Security Priorities and Investments

Top priorities include improving regulatory compliance, boosting security education and preventing and detecting breaches. Top investments for the year ahead are an audit tool or log management system, a data loss prevention system and a mobile device management system.

5. BYOD Widespread, But are Protections Keeping Up?

A majority of organizations allow clinicians to use personal mobile devices for work-related purposes. But mobile security policies are still evolving.

6. Cloud Computing: Concerns Persist

Most healthcare organizations are not yet using cloud computing. Why? They're concerned about enforcing security policies and HIPAA compliance.

Flashback: A Look at the 2011 Survey Results

The inaugural edition of the Healthcare Information Security Today Survey in 2011, like the latest edition, found that top priorities were boosting regulatory compliance and improving security education.

As healthcare organizations continue their efforts to keep patient information private when adopting electronic health records and exchanging patient data, it's no surprise that complying with the HIPAA privacy and security rules and educating staff about the role they play in data security continues to be at the top of the agenda.

In the 2011 survey, top security investments on the horizon were audit logs, mobile device encryption and data loss prevention. In the new survey, audit tools and DLP remain at the top of the list, but mobile device management systems are now a top priority as well, reflecting increasing concerns about the rapid growth in the use of smart phones, tablets and other next-generation devices.

The 2011 survey found that 26 percent of organizations had yet to conduct a risk assessment, as mandated under HIPAA. In contrast, the new survey shows that only about 8 percent had not conducted an analysis, a significant improvement. But are organizations keeping their assessments current to reflect current threats? In the new survey, nearly a third of organizations say they have not conducted a risk assessment in the past year.

When it comes to information security spending trends, the two years' worth of survey results show no momentum toward increased spending. The 2011 survey showed 43 percent expected an increase in spending, while the new survey shows only 37 percent expect an increase in the year ahead.

1. Breach Prevention: Emerging Priorities

The second annual Healthcare Information Security Today survey takes a close look at breach prevention trends.

Publicity about major health information breaches, as well as hefty federal fines for HIPAA non-compliance tied to several breach investigations, are major catalysts for information security investments. The survey confirms that preventing and detecting breaches is one of the top three security priorities for the coming year, along with improving regulatory compliance and boosting security training.

The final HIPAA Omnibus Rule, which was released in January 2013, officially increases the penalties for HIPAA non-compliance and spells out a ramping up of HIPAA enforcement efforts. It also includes a new breach notification rule that greatly clarifies how to assess whether a breach must be reported.

The Omnibus Rule compliance deadline looms in September 2013. Also on the horizon is the resumption of the federal HIPAA compliance audit program later this year or early in 2014.

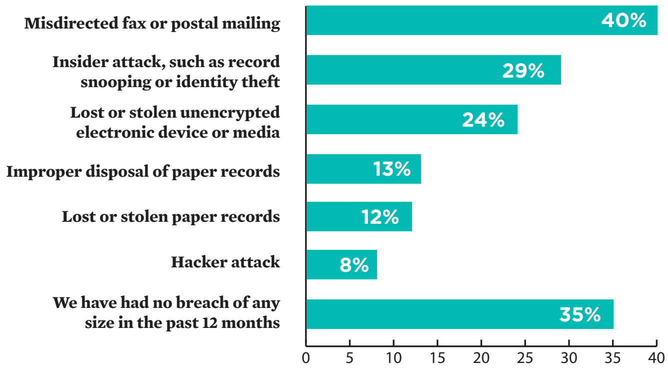
The perception that federal regulators are finally getting serious about enforcing HIPAA could prove to be a powerful incentive for ramping up security investments in the years to come. But for now, the 2012 survey results show there's plenty of work yet to be done.

Since September 2009, when an interim version of the breach notification rule went into effect, federal officials have confirmed more than 540 major breaches affecting a total of more than 21.5 million individuals. The tally for smaller breaches (affecting 500 or fewer individuals) stood at more than 60,000 through the end of 2011.

Given government statistics that show breaches are widespread, it's somewhat surprising to see that 35 percent of survey participants believe they have not experienced a breach of any size within the past 12 months, and nearly 60 percent say their business associates have not experienced a breach in that period. This could be a reflection of insufficient breach detection efforts as well as a failure of business associates to inform their partners about incidents.

"I'm sure there are lots of breaches that go unreported," says security consultant Tom Walsh. "If you think you are in great shape because no breaches are being reported, you may want to go back and do a little closer look. Perhaps your employees or your workforce members don't even know that something is a reportable event. Or maybe they don't know how to report it."

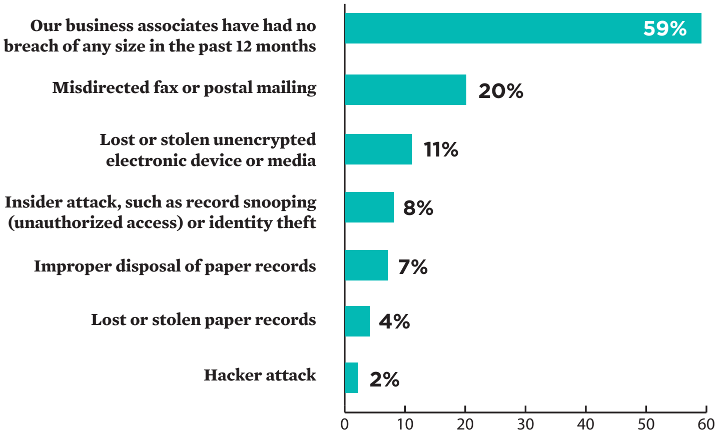
What type of health information breach (of any size) has your organization experienced in the past 12 months?



ULTIMATE AUTHENTICATION ENGINE

Driven by insight and risk-based analytics with RSA® Authentication Manager 8.0.

What type of health information breach (of any size) has a business associate(s) with access to your organization's patient information had in the past 12 months?



So what steps are organizations taking to prevent breaches? The survey shows top priorities are stepping up training, implementing encryption of mobile devices and removable media, and installing an audit tool to enhance detection of unauthorized access.

Walsh suggests that one important breach prevention strategy is to issue encrypted USB drives and encrypted external portable hard drives for secure storage of information. Such a move could be paired with the use of virtualization, he says. That involves storing data on servers inside a secure data center, rather than on PCs.

The survey shows that the most common action taken as a result of a breach is changing data security/privacy strategies and procedures, followed by launching of an awareness/training program.

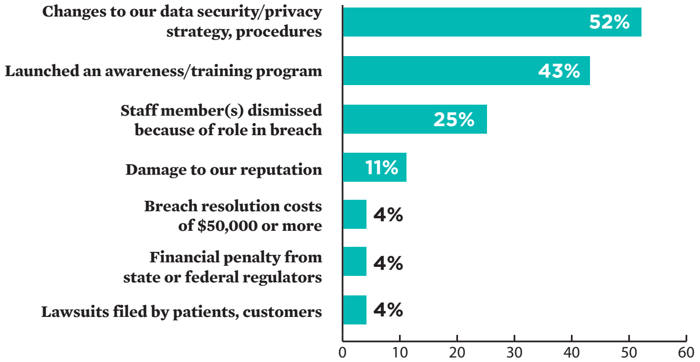
"The key here in changing your procedures is to actually do what you say," Walsh stresses. "There are a lot of policies in healthcare that have been developed that address many of the issues, but people aren't actually taking the time to read them."

> I'm sure there are lots of breaches that go unreported. ”

Hospitals, clinics and others should make sure that all staff members – and even volunteers – who have access to patient information are familiar with all privacy and security policies.

An effective training program is essential, Walsh stresses. Staff should be tested on privacy and security issues before and after training to measure its effectiveness, he adds. One particularly effective form of training, Walsh says, involves videos featuring employees. This approach helps make the messages more memorable, he argues.

If your organization or a business associate has had a breach in the past 12 months, what was the impact?

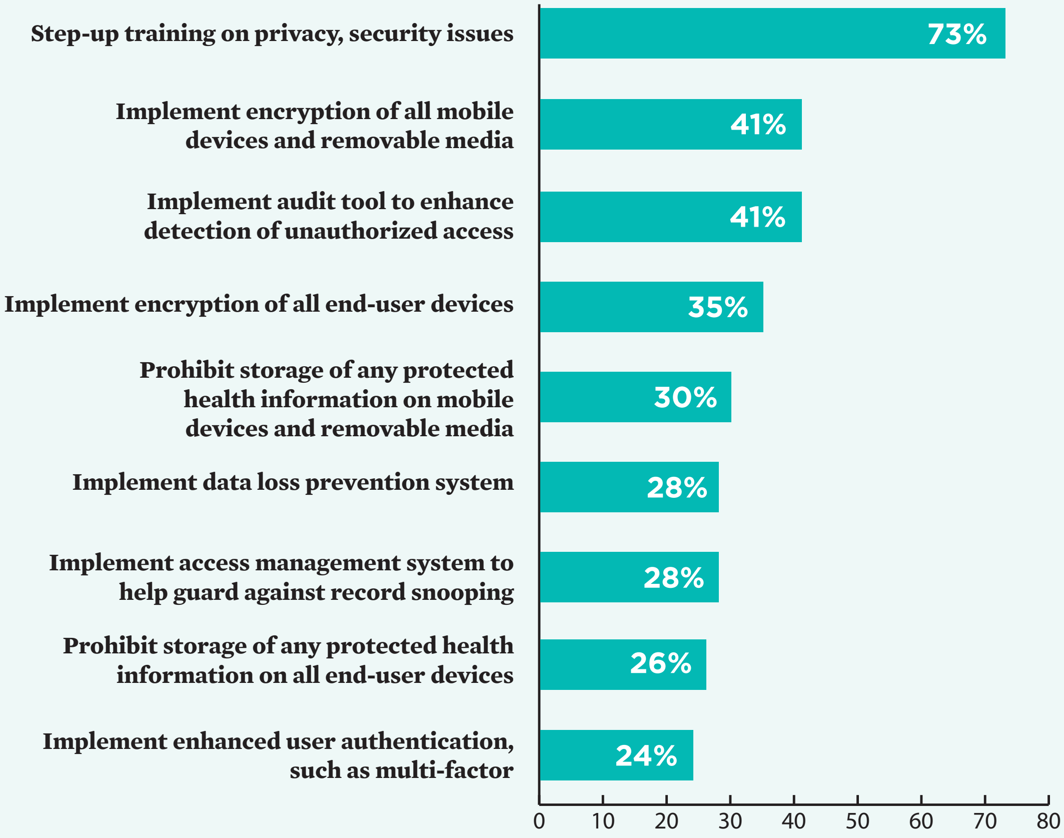


The biggest perceived security threats, the survey shows, are mistakes by staff members, the growing use of mobile devices and business associates taking inadequate security precautions.

These survey results reinforce trends seen in federal breach reports. A majority of the major breaches listed on the HHS "wall of shame" were caused by lost or stolen devices or media, with misplaced laptops a common cause. Plus, more than 20

Survey Spotlight: Breach Prevention

What steps does your organization plan to take in the coming year to help prevent health information breaches?

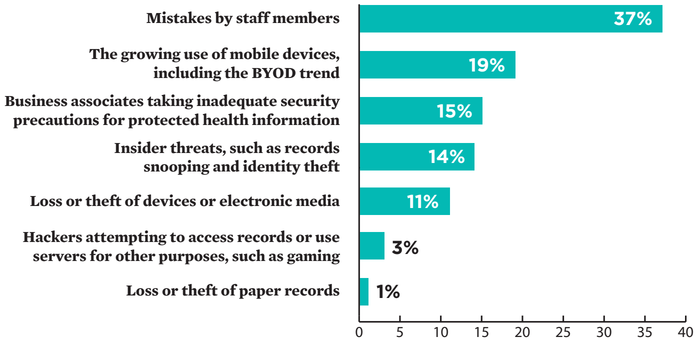


> The key in changing your procedures is to actually do what you say.

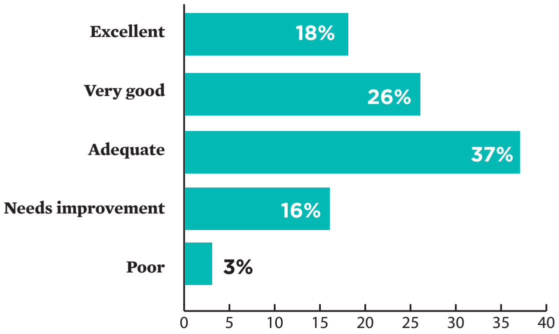
percent of major breaches have involved a business associate. The survey shows healthcare organizations are more confident about their ability to counter external threats than they are about countering internal threats.

Considering the major causes of breaches listed in the survey, that's no surprise. While hacker attacks are rare, breaches tied to internal issues, such as misdirected faxes and mailings, records snooping, identity theft and lost/stolen devices are far more common. The same pattern is true of breaches at business associates.

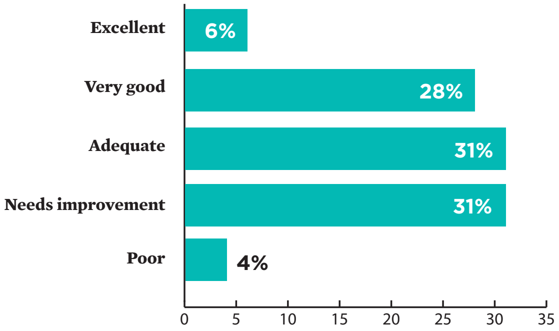
What do you perceive to be the single biggest security threat your organization faces?



How would you grade your organization's ability to counter EXTERNAL information security threats?



How would you grade your organization's ability to counter INTERNAL information security threats?



> Business associates should be required to provide some type of evidence or proof of compliance to their covered entities.

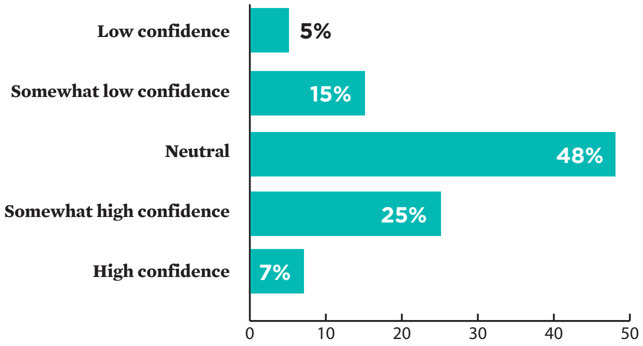
Only 32 percent of survey respondents express confidence in the security controls maintained by their business associates.

A large majority of healthcare organizations have modified business associate agreements to provide more details to help ensure patient information is adequately protected. But less than one-third have required their business associates to complete a security questionnaire or asked for a copy of their security policies or audits. Rarer still is third-party validation of business associates' policies and procedures.

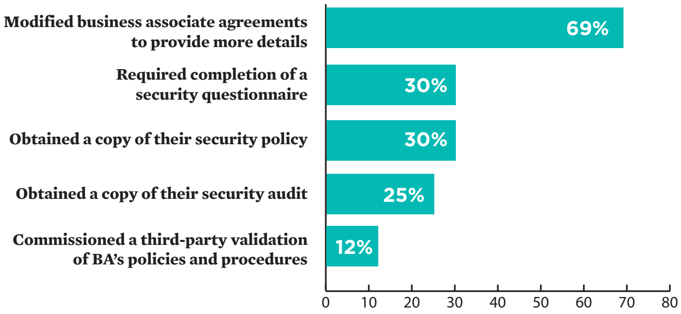
For years, healthcare organizations have relied on their business associate agreements as a primary way to help make sure their vendor partners are taking adequate security precautions. But the new HIPAA Omnibus Rule released in January 2013 clarifies that business associates and their subcontractors have direct responsibility for HIPAA compliance – and they face potential penalties for failure to comply.

"Business associates should be required to provide some type of evidence or proof of compliance to their covered entities," Walsh says.

How would you rate your confidence in the security controls maintained by your business associates and their subcontractors?



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

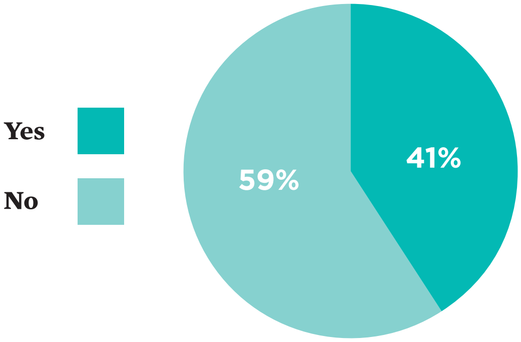


Despite all the publicity about major breaches, almost 60 percent of organizations do not have a portion of their IT budget allocated for breach detection, response and notification costs.

And even though an interim final version of the HIPAA breach notification rule went into effect in 2009, 40 percent still don't have a detailed plan in place to comply with the rule. Of those with a plan in place, more than half have yet to test it.

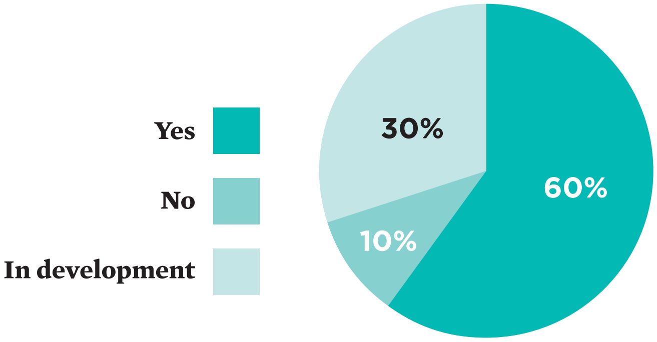
With the recent release of a final version of the breach notification rule, perhaps organizations will ramp up their compliance efforts and devote more resources to breach prevention. The new breach notification rule, included in the HIPAA Omnibus Rule, greatly clarifies how to conduct a risk assessment to determine whether a security incident merits reporting to federal authorities and the patients affected.

Does your organization have a portion of its IT budget specifically allocated for information breach detection, response and notification costs?

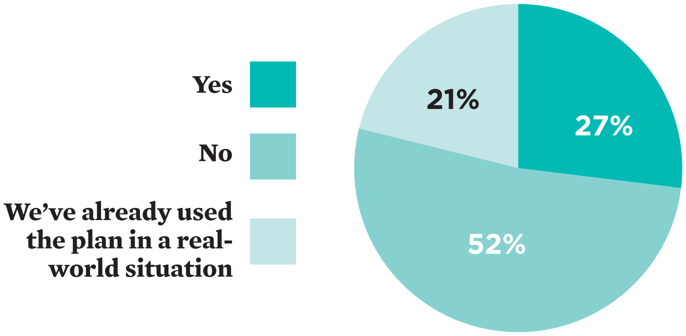


> With the recent release of a final version of the breach notification rule, perhaps organizations will ramp up their compliance efforts and devote more resources to breach prevention.

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

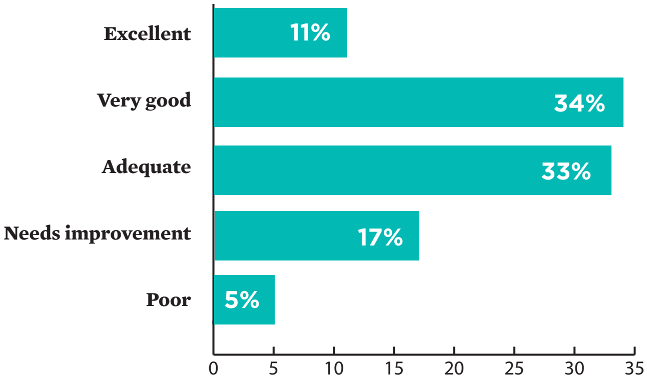


If you have a compliance plan in place, has your organization conducted a test to see if the breach notification plan will work in a real breach situation?

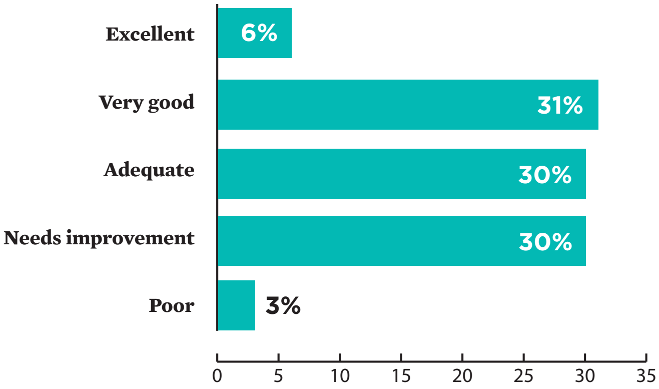


Despite all the work left to be done to prevent breaches, a substantial majority of organizations surveyed say their ability to comply with HIPAA and HITECH privacy and security requirements is adequate or better. But a third say they've still got plenty of work to do on improving security training.

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



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



ANALYSIS

Working With Business Associates to Prevent Breaches

Tom Walsh, President, Tom Walsh Consulting

HEALTHCAREINFOSECURITY: What do you see as the best ways to help ensure business associates take all appropriate breach prevention steps?

TOM WALSH: I believe that business associates should be required to provide some type of evidence or proof of [HIPAA] compliance to their covered entities. I've been tracking the breaches that get reported to the Department of Health and Human Services on their website, and what I find is approximately 20 percent of the breaches are caused by business associates. And keep in mind, those breaches that are caused by your business associate are not going to be covered by the cyber-insurance that a covered entity might have.

So it is important ... that you know that there is reasonable assurance that they are doing the right things. It could be in the form of a letter from a third-party that conducted some type of independent evaluation and validation of the business associate's safeguards and controls. And it should look at both technical and non-technical review.

One of the things that I'm recommending is that you use the HIPAA audit protocol as guidance for conducting that type of an assessment. This HIPAA audit protocol was released by the Office for Civil Rights. It is actually the audit procedures being used for the audits being conducted. So, while the protocol is written for covered entities ... if a business associate could meet it today, I think that should give covered entities a great deal of confidence that their data is being protected. ...

> Approximately 20 percent of the breaches are caused by business associates.
>
> - TOM WALSH

HEALTHCAREINFOSECURITY: About 60 percent of organizations do not have a portion of their IT budget allocated specifically for breach detection, response and notification costs. And about 40 percent do not have a detailed plan in place to comply with the HIPAA breach notification rule. On the other hand, preventing and detecting breaches is one of the top three security priorities for the year ahead. So what is your reaction to these results?

WALSH: My initial reaction is that this is kind of human nature. The results really reflect our general attitude toward any kind of "what-if" planning. We don't want to think about what bad things can occur, so we tend to try to put it off. And we're dealing with a lot of issues right now in healthcare just trying to keep physicians happy. ... So doing the what-if planning takes a lower priority.

And I've seen this not just in breach planning, but also in disaster recovery planning, where there are a lot of outdated plans ... I noticed again in the survey that about 20 percent of the people who responded said they were planning to develop a breach detection and notification plan this year, which is good. But you really need to test your plan too. ... You want to make sure that your plan works.

Tom Walsh, CISSP, is president of Tom Walsh Consulting, an independent consulting firm based in Overland Park, Kan., that advises healthcare organizations on information security. Walsh is a nationally recognized speaker and also the co-author of books on healthcare information security published by the AMA, AHIMA and HIMSS.

2. Encryption and Authentication: A Long Way to Go

Encryption and authentication can play critical roles in preventing breaches. But the survey confirms that healthcare organizations still have a long way to go in implementing these technologies.

As mentioned earlier, top breach prevention steps organizations plan to take in the year ahead include encryption of all mobile devices and removable media (41 percent) and implementing encryption for all end-user devices (35 percent).

The survey poses the open-ended question: "What one factor would most improve information security at your organization?" The most common answer? Encryption.

Other survey results illustrate why encryption is on the wish lists of many security professionals. For example, about two-thirds of organizations encrypt information sent across external networks, and 58 percent encrypt mobile devices. So some organizations still have plenty of work to be done in ensuring secure communication and addressing the cause of many breaches – the loss or theft of unencrypted mobile devices. Meanwhile, only about half encrypt backup tapes, desktop PCs, mobile storage devices or servers/databases.

"I think we are going to see increasing use of encryption over time," says Eric Cowperthwaite, CISO at Providence Health and Services, a delivery system based in Seattle.

Walsh, the consultant, says more hospitals need to focus on secure communication with physicians. "A lot of organizations have their outbound e-mail encryption in place. ... But what I'm talking about is what happens to the data after the recipient receives it, in particular if any attachments are sent. Where does that get stored? How is that protected?

> Part of the problem is that folks in the healthcare industry have chosen to have the same authentication approach for all of the various use cases.

Hospitals and clinics also need to make sure physicians aren't using text messaging inappropriately, putting sensitive patient information at risk, Walsh notes.

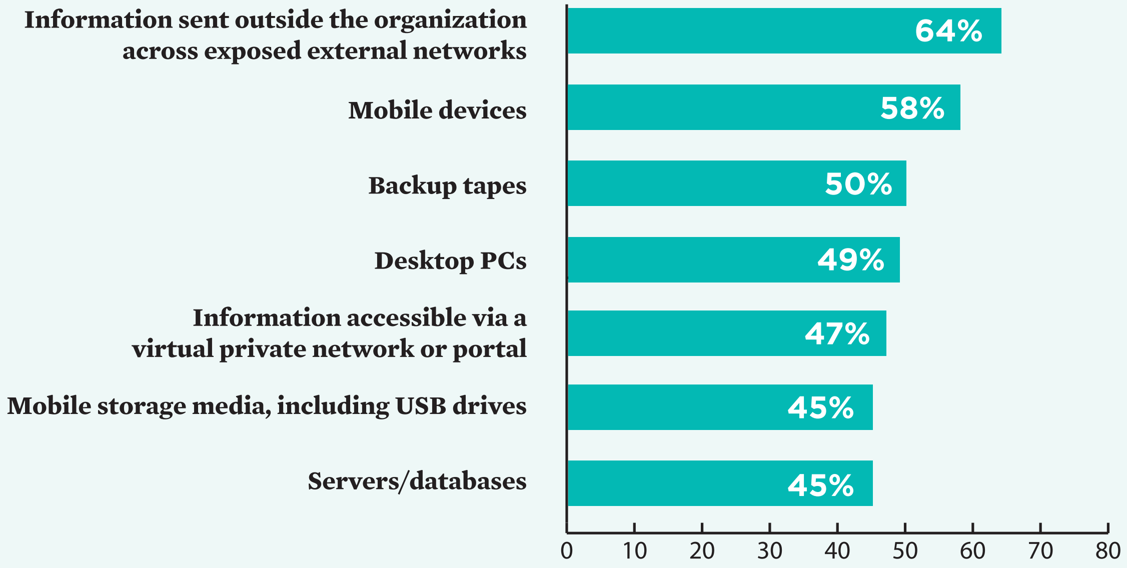
Using strong authentication to verify the identities of healthcare staff members who access patient records can play an important role in preventing inappropriate access to confidential information. But the use of authentication beyond username and password is relatively rare, the survey shows.

For example, 21 percent are using digital certificates and 16 percent are using one-time passwords with two-factor authentication, such as a token of some sort.

Survey participant Mark Combs, CISO at WVU Healthcare in Morgantown, W.Va., notes: "Passwords, especially weak passwords, are probably one of the biggest threats to organizations. There are users who share them, who fall prey to social engineering and who leave them written on pieces of paper near their workstation. Implementing a stronger authentication method, albeit one that would not impact provider workflows, could immediately strengthen our security posture."

Survey Spotlight: Encryption

Specify whether your organization currently applies encryption for:



Survey participants were asked: What one factor would most improve information security? The most common answer: Encryption.

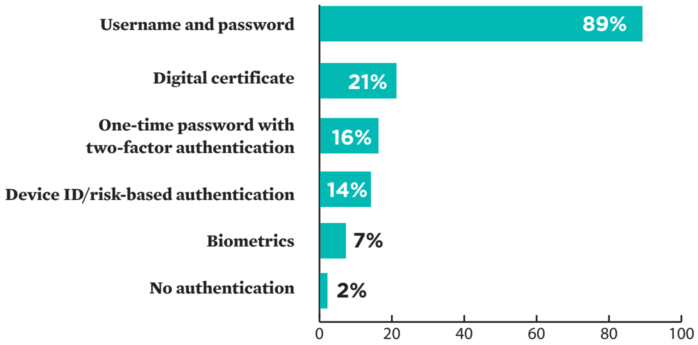
What's the best type of authentication to use? That depends on how and where clinicians are accessing patient records, says Cowperthwaite, the Providence Health CISO. For example, stronger authentication is needed for a physician accessing records remotely from their office than for a nurse logging onto a workstation at the hospital, he contends.

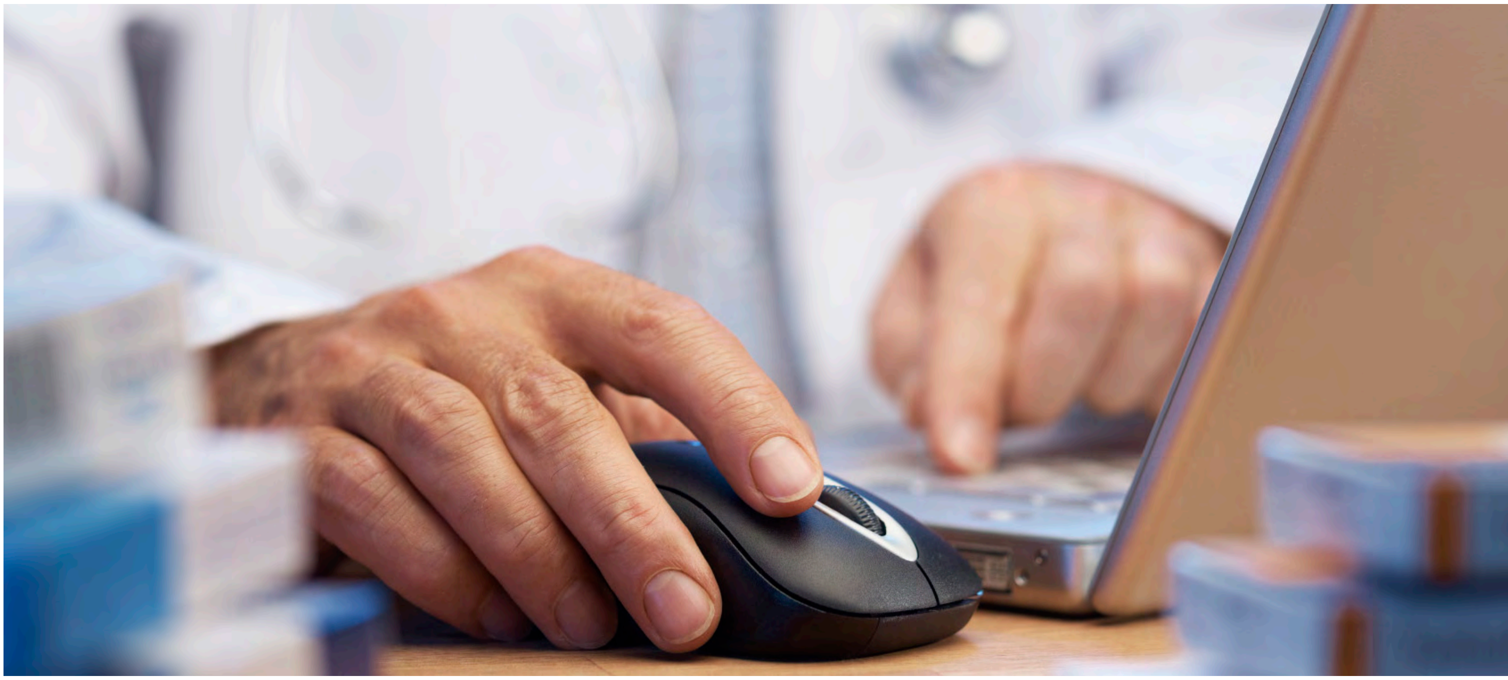
"Part of the problem is that folks in the healthcare industry have chosen to have the same authentication approach for all of the various use cases, rather than looking at the different use cases, the risks involved, and what will be appropriate to manage and control those risks," Cowperthwaite says.

One reason stronger authentication isn't more common, the CISO argues, is that "there hasn't been very much evidence presented to healthcare organizations yet that inappropriate access by malicious actors is a big problem, except for internal snooping. We aren't seeing evidence yet that bad guys are out there trying to break into our EHRs and harvest patient information. ... If there are some well-publicized breaches, then we're going to start seeing a changing set of attitudes about this."

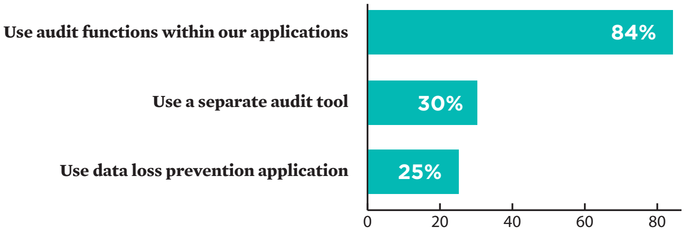
And when it comes to tracking who actually accesses sensitive information, the survey shows a strong reliance on the audit functions within applications, such as electronic health records systems, rather than a separate audit tool or data loss prevention application.

To guard against inappropriate access to electronic health records, what type of authentication does your organization require for users to gain access while they are on the job at one of your facilities?





How does your organization track who accesses protected health information?



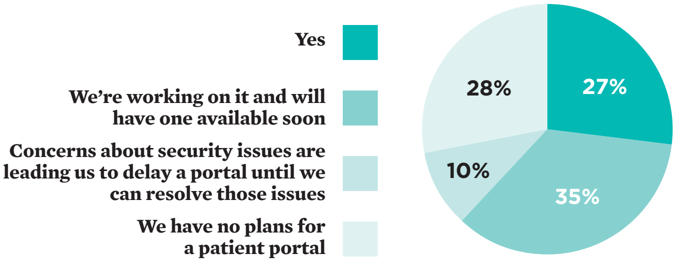
The survey shows only 27 percent of organizations are offering patients access to certain records through a portal, but 35 percent have a portal in the works. Authentication will be a big challenge in this arena as organizations take steps to ensure that the right patients get access to the right information.

Healthcare organizations could look to the knowledge-based authentication experiences in online banking for guidance in this arena, Cowperthwaite notes. This approach would rely on asking patients a series of personal questions and verifying the accuracy of the answers.

“We should be looking at what other industries have done when they needed to create customer portals,” Cowperthwaite says. “They likely have worked the bugs out and have made them effective and have found the balance between appropriate security and ease of access.”

> We should be looking at what other industries have done when they needed to create customer portals.

Does your organization offer a web portal that patients can use to complete such tasks as obtain test results, access certain records or make an appointment?



ANALYSIS

Breach Prevention: The Role of Encryption

Eric Cowperthwaite, CISO, Providence Health and Services, Seattle

HEALTHCAREINFOSECURITY: When it comes to steps that organizations plan to take this year to prevent breaches, 41 percent mention encryption of all mobile devices and removable media, while 35 percent mention implementing encryption for all end-user devices. With all the publicity about breaches involving lost and stolen devices, is the healthcare industry finally moving toward more universal use of encryption?

ERIC COWPERTHWAITE: We are going to see a continued increasing use of encryption over time. The default standard practice... is going to be to encrypt any device that contains patient data and could leave your physical control. Since about 2006, we have required that all devices that leave a Providence facility and contain confidential data be encrypted. So essentially, all laptops, tablets, back-up tapes that go offsite have been encrypted since 2006. We've created criteria for determining risk related to the loss of desktop devices and have encrypted any of those that were determined to pose a high risk. So essentially, any desktop that contains patient data that would meet the threshold of having to report to HHS if it were stolen has been encrypted.

HEALTHCAREINFOSECURITY: Our survey also finds that 65 percent encrypt information that is sent outside their organization across exposed networks, and 58 percent now encrypt mobile devices. Why aren't those numbers higher?

> The default standard practice ... is going to be to encrypt any device that contains patient data and could leave your physical control.
>
> - ERIC COWPERTHWAITE

COWPERTHWAITE: One thing that we ought to think about is the survey included many different types and sizes of healthcare organizations, and I suspect that the small clinics are not doing that sort of thing right off the bat. ... So some of it is about the organization size and scope and then some of it has to do with the fact that mobile devices as a means of managing and transmitting confidential data is a pretty new thing. ... We've only been talking about mobility as a significant issue and strategy for the last couple of years. ...

HEALTHCAREINFOSECURITY: A smaller percentage of those surveyed are applying encryption to back-up tapes, desktop PCs, mobile storage media and servers. How should organizations go about prioritizing encryption projects?

COWPERTHWAITE: Security programs in healthcare, according to the HIPAA Security Rule and the HITECH Act, are supposed to be risk-based, and they are supposed to be appropriate to the size and scope of the organization and the risk the organization faces. So I think we should go with that as the starting point about deciding whether you're going to encrypt your back-up tapes ahead of your desktop PCs, as an example. ... The first thing we did a couple of years ago when we decided that we needed to move beyond encrypting laptops and tablets was to do ... an assessment of our risk. And that gave us an opportunity to prioritize what we should do first, and I think that is what people need to do.

Eric Cowperthwaite is CISO at Providence Health and Services, a Seattle-based system with 27 hospitals.

Listen to this interview:
http://www.healthcareinfosecurity.com/interviews.php?interviewID=1765

3. Risk Assessments: Keeping Up Is a Challenge

Several recent high-profile settlements in cases involving HIPAA non-compliance have called attention to the importance of conducting risk assessments and then taking action to mitigate risks identified. The HHS Office for Civil Rights, after investigating several data breaches, has issued hefty financial penalties for organizations that lacked a current risk assessment, which could have helped prevent the incidents.

HIPAA and the HITECH Act both require current risk assessments. Yet the survey shows about one-third of organizations have not conducted an assessment within the past year. Of those with updated assessments, two-thirds say the analysis was prompted, at least in part, by participation in the HITECH Act electronic health record incentive program. And more than half got outside help with their assessment.

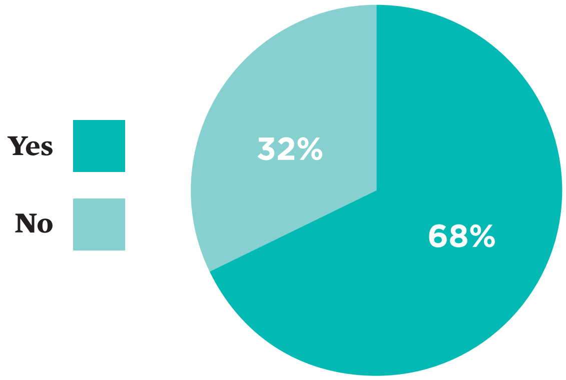
"A security assessment should be conducted periodically and it may be more rigorous one year than the next, but it certainly should be updated annually," says Bill Spooner, CIO at Sharp Healthcare, a San Diego-based delivery system. "And there should be a plan in place to address the higher risk areas."

Sharp conducts an internal risk assessment and also uses an outside firm "that takes a look at our risks and helps us really balance the approach that we're taking," Spooner notes. "And whereas we don't do a ground-up assessment every year, we update what we've seen in the prior year. We look at the results of the various audits that we've done during the course of the year and we identify where we need to make course corrections. The environment is just too dynamic to believe that you wouldn't want to update it annually. ... As you recognize that new threats are coming to you in the security environment, you'd better be thinking about how you're responding to them."

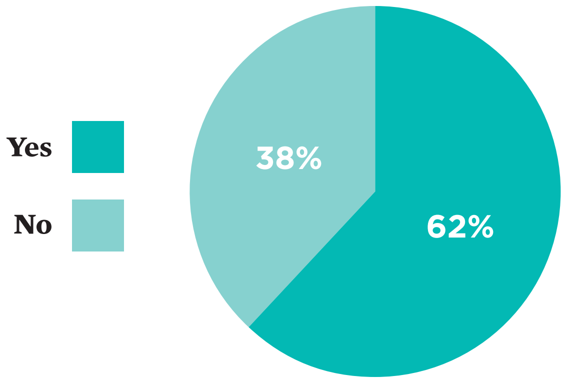
The survey also shows that for those with an updated risk assessment, the most common action taken as a result of the analysis is revising and updating security policies, followed by implementing new security technologies.

Once they put security controls in place, how do organizations measure if they're effective? An internal risk analysis and an internal audit are, by far, the most common approaches, with an external risk analysis mentioned less frequently.

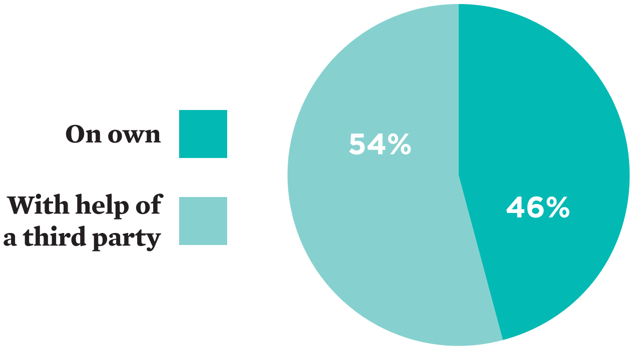
Has your organization conducted a detailed information technology security risk assessment/analysis within the past year?



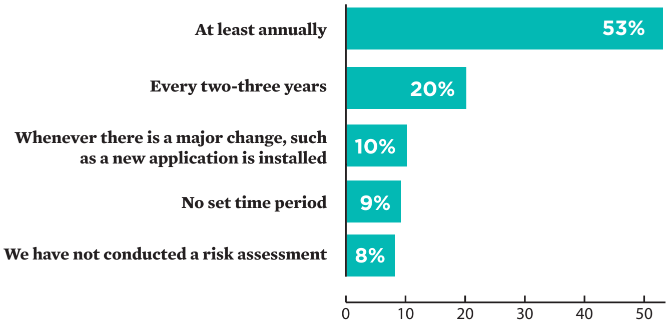
If your organization has conducted a risk assessment within the past year, was your organization's most recent risk assessment triggered, at least in part, by its participation in the HITECH Act electronic health record incentive program?



If your organization has conducted a risk assessment within the past year, did your organization conduct the risk assessment on its own or with the help of a third party?

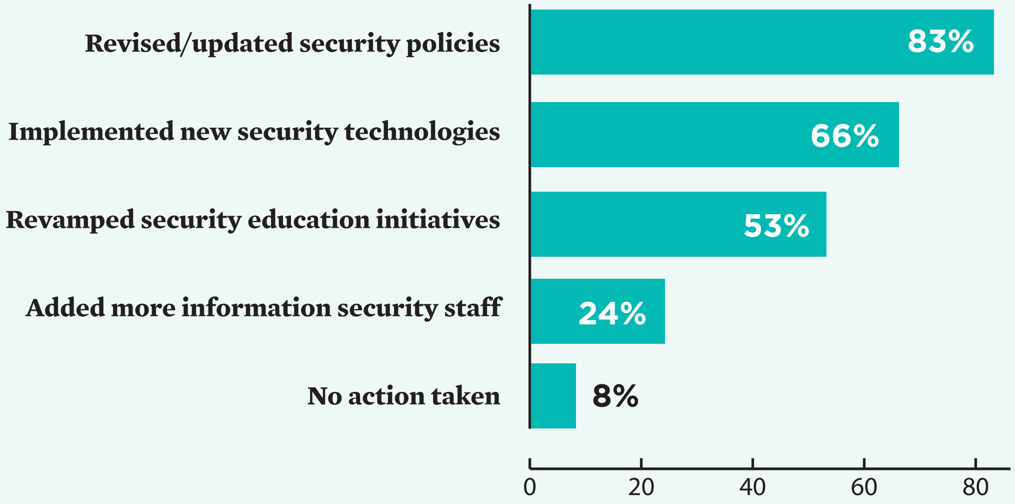


How often does your organization update its risk assessment?



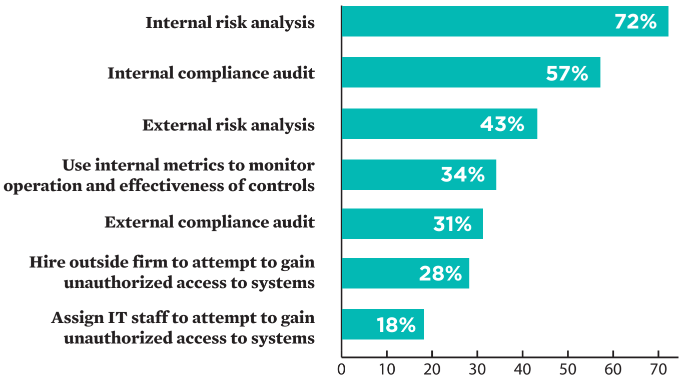
Survey Spotlight: Results of Risk Assessment

If your organization has conducted a risk assessment within the past year, what action has it taken as a result of its assessment?



> A security assessment should be conducted periodically and it may be more rigorous one year than the next, but it certainly should be updated annually.

How does your organization measure/monitor whether its security controls are working?



> As you recognize that new threats are coming to you in the security environment, you'd better be thinking about how you're responding to them. ”

4. Top Security Priorities and Investments

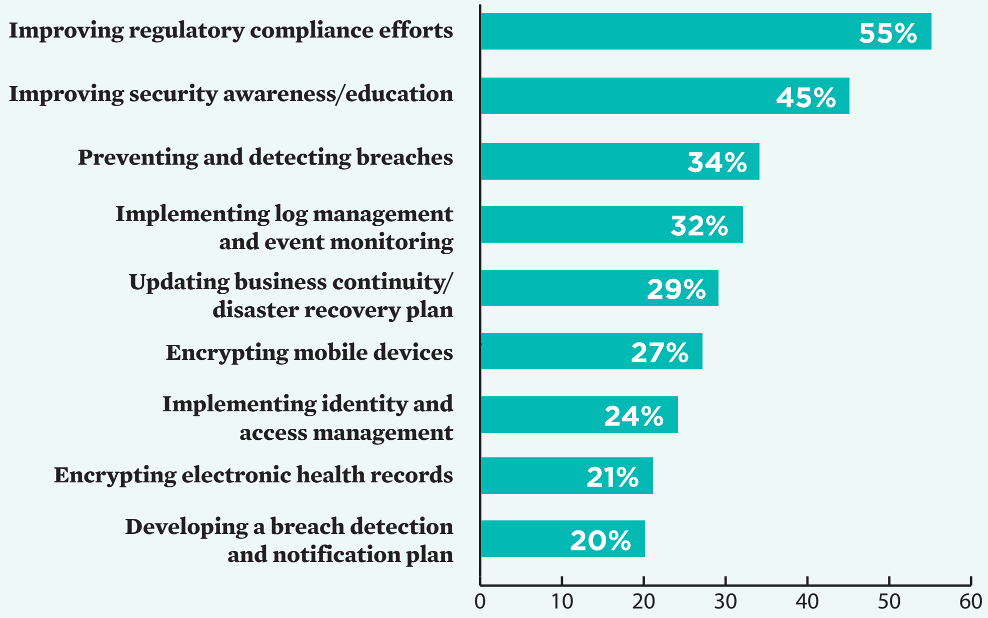
The survey shows the top information security priorities for the coming year are improving regulatory compliance and improving security education – the same as in the 2011 survey. Preventing and detecting breaches is the No. 3 priority in the latest survey, up from No. 5 in 2011.

These top three priorities clearly are interrelated. For example, improving HIPAA compliance and educating staff about HIPAA can help prevent breaches.

“When you recognize that almost every week there is some kind of a reported breach around the country involving thousands of patient records being potentially compromised, and the fines and other punishment plus the poor public relations that go with that, it’s really increasing the emphasis, rightfully so, on improving our security profiles,” says Spooner, the CIO at Sharp Healthcare. “And when you add on top of that the fact that the technology is changing all the time, [and we’re] getting different kinds of attacks that we need to protect against, we have to continue to raise our game just in the same way that hackers are raising theirs.”

The survey shows top technology investments for the year ahead are an audit tool or log management system, a data loss

What are your organization’s top three information security priorities for the coming year?



> Mobile device management is a huge issue if you want to enable a mobile workforce and all of the benefits that it entails.

prevention system and a mobile device management system. These technologies all can contribute to breach prevention efforts.

Cowperthwaite of Providence Health sees a mobile device management system as essential. "In an organization like mine, where we have 65,000 employees, 3,000 of whom are employed physicians, and we have many thousands of affiliated healthcare providers, we are seeing literally tens of thousands of mobile devices. Having a way to know who has what device, how it is connected to our networks, how it's protected, what sorts of applications are on it, what its life cycle is ... is very important. ... Mobile device management is a huge issue if you want to enable a mobile workforce and all of the benefits that it entails."

The survey shows that, in many cases, the resources available for information security are limited. Only 37 percent expect their budgets for information security to increase in the year ahead. And when it comes to spending for information security, the most common answer is that 1 to 3 percent of an organization's IT budget is devoted to security.

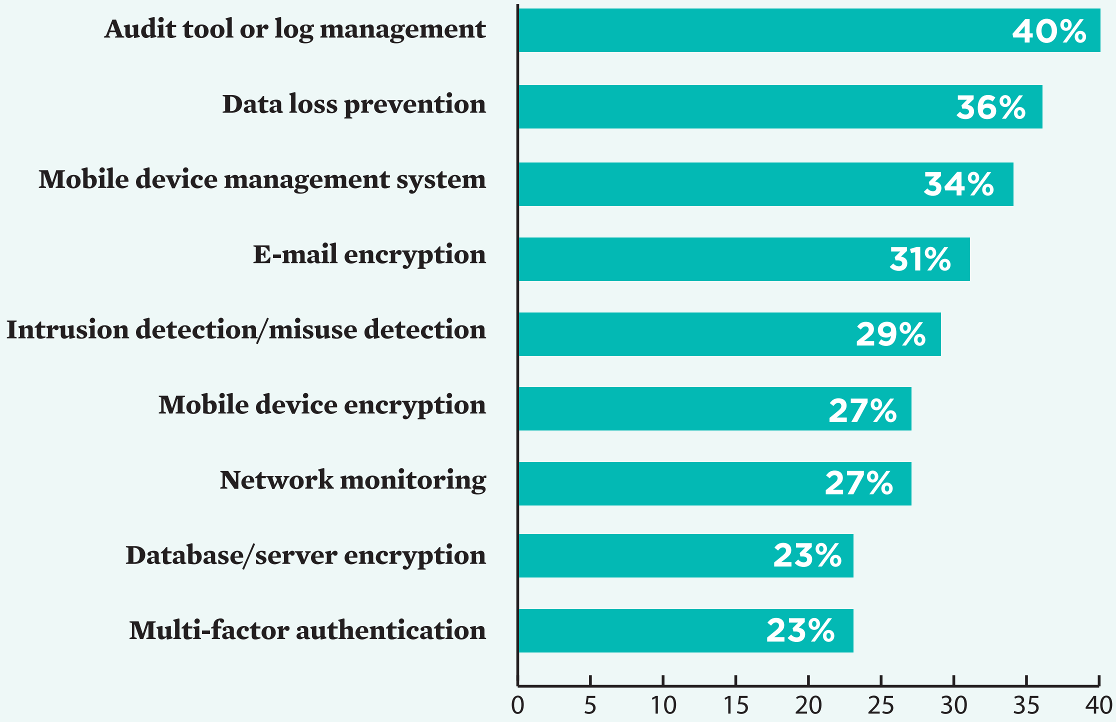
The most common way to obtain funding for information security is to ask for money to be allocated out of the overall IT budget as needed for security projects, the survey shows.

Also, only 44 percent report they have a documented information security strategy. And 70 percent have a full-time chief information security officer.

"The reason that I believe it is difficult to win support for investing in security is the balance between ease of use, employee productivity and patient care," says Spooner, the CIO at Sharp. "To ask a clinician to use a larger password or to have to go through additional steps in terms of authenticating themselves on the system or to do other things that they would

Survey Spotlight: Tech Investments

Which of the following technologies does your organization plan to invest in next year?



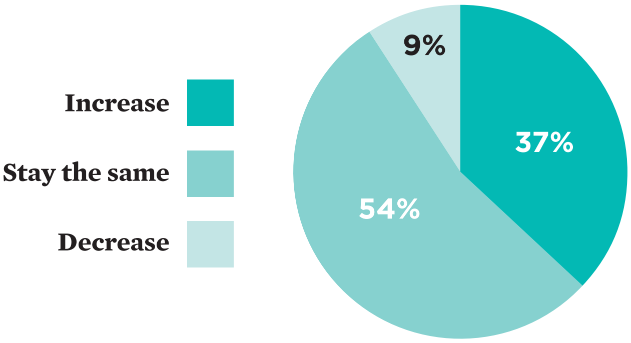
> The reason it is difficult to win support for investing in security is the balance between ease of use, employee productivity and patient care.

believe slows down their work in terms of taking care of patients meets resistance."

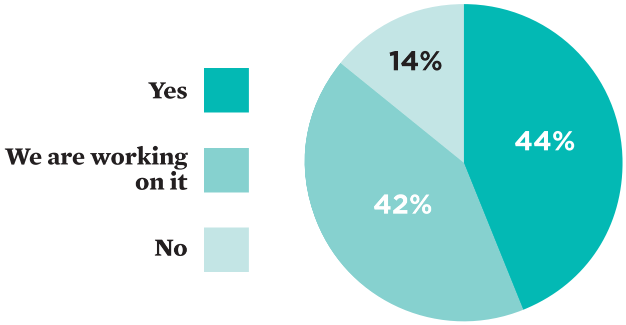
Unfortunately, the key to winning senior executive support for ramped-up security spending, Spooner says, "is to have a breach or have your neighbor have a breach. ... Typically, the organization that has the breach finds themselves implementing more rigorous procedures – things that they probably should have had in the first place. ... But with the number of reported breaches that we're seeing in the news almost every week, it's not quite as difficult of an argument as it was five or 10 years ago, because we realize that we're all vulnerable."
Regarding budgeting for information security, Spooner argues that it's natural that security be part of the overall IT budget "because we have security ingrained in many aspects of our operations."

But just as important as spending levels is the commitment to security at the highest levels, Spooner says. "I believe that the leadership commitment is, in many ways, more important than the absolute amount of money that you're spending on it. For certain, you have to have tools to monitor, track, ensure that you're having good security. But I'm not sure that another X number of dollars makes your security that much better as compared to commitment from leadership that security is important."

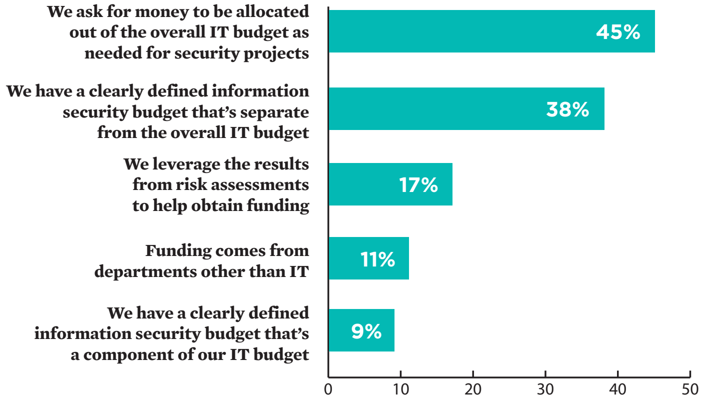
Will your organization's budget for information security next year:



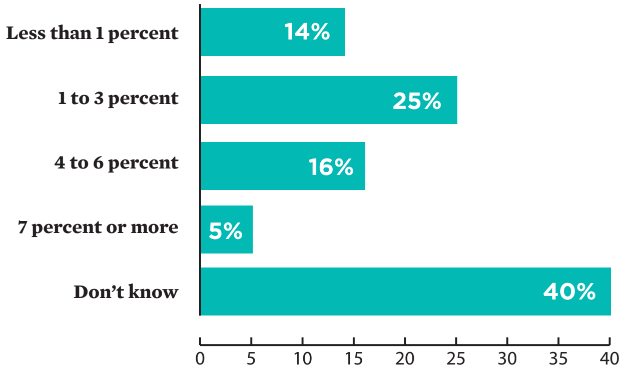
Does your organization have a documented information security strategy?



How does your organization fund information security?



What percentage of your organization's total IT budget for the coming year will be devoted to information security?



ANALYSIS

Information Security Priorities for the Year Ahead

Bill Spooner, CIO, Sharp HealthCare, San Diego

HEALTHCAREINFOSECURITY: The survey shows that the top three information security priorities for the coming year are improving regulatory compliance efforts, improving security awareness and education and preventing and detecting breaches. What do you think of this list?

BILL SPOONER: Well I think that the priorities are right in line with our thinking here at Sharp. ...

On top of the three priorities that you mentioned that came out of the survey, one of our priorities additionally this year is implementing a more formalized governance, risk and compliance program. That is a series of processes to ensure that we're evaluating risks around new applications and new processes to ensure that we're looking at these things consistently and that we are thoughtfully assessing the risk of whatever we do in terms of our IT program and related processes so that we feel defensible and comfortable in terms of the level of risk that we're taking. Along with that, we're putting in a computerized tool set to facilitate the analysis and track the decisions that we make. That along with the three priorities that you mentioned are pretty important to us.

HEALTHCAREINFOSECURITY: When we ask about security technology investments for the year ahead, the top responses are audit tool or log management, data loss prevention, and mobile device management systems. Tell us about the investments that Sharp plans to make.

> Like many organizations, we are implementing a mobile device management product that includes a security suite.
>
> - BILL SPOONER

SPOONER: Well I already talked about the investment in GRC. But in addition to that we are raising our game in a couple of areas.

We're implementing a data scrambling tool for our non-production environments where we want to ensure that we're not using real patient data as we're testing applications.

Like many organizations, we are implementing a mobile device management product that includes a security suite to help secure mobile devices, recognizing that we are seeing more and more requests to use iPads and other similar mobile devices on our system. We really need to ensure that we're providing adequate protection around that.

We're upgrading our wireless infrastructure to some extent to better segment the mobile device traffic out of the internal network. We are improving our logging system so that we're tracking activity ... We're also looking to implement a newer clinical auditing tool that is a little bit more comprehensive than the product that we're using today.

Bill Spooner is CIO and Sharp HealthCare, a San Diego-based delivery system with seven hospitals.

Listen to the interview:
http://www.healthcareinfosecurity.com/interviews.php?interviewID=1866

5. BYOD Widespread, But Are Protections Keeping Up?

A majority of organizations surveyed say they allow clinicians to use personal mobile devices for work-related purposes. Of those that permit BYOD, about half prohibit storage of patient information on the devices and require strong passwords, the use of an automatic time-out function and the installation of remote wiping capability on the devices. Some 46 percent require encryption of the devices.

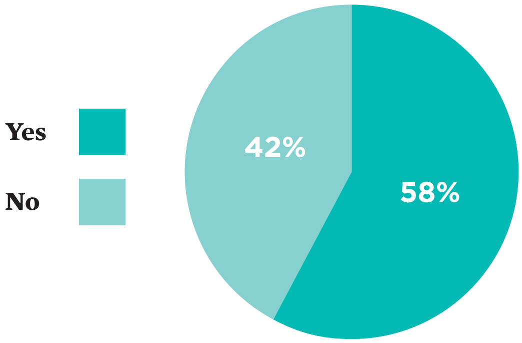
When it comes to their broader mobile security policies, more than half prohibit storage of patient information on the devices and apply encryption. Some 11 percent still lack a mobile security policy.

For those who provide clinicians with remote access to clinical systems, the most common security measures are using a virtual private network and encrypting all information accessed remotely.

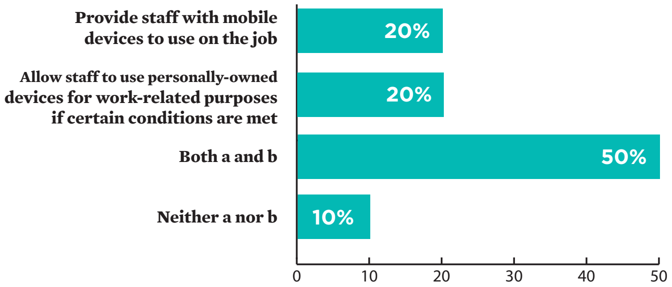
In addition to establishing a clear-cut policy spelling out acceptable uses of personally owned mobile devices, hospitals and other organizations "need to then create processes to enable employees to do what the policy says they can do," Cowperthwaite says. "So if we say that they can use their own personal mobile device as long as that use has been authorized by their manager, then we need to build a process so that they can request it, the manager can approve it, and it can be handed over to IT for whatever technology [installations] have to happen."

Cowperthwaite says that technical controls are essential. "If you've decided that confidential information can be on those devices so long as they are encrypted, password protected and can be remotely wiped, and the employee understands reporting procedures when the device is lost or stolen ... then you need a set of technical controls that enforce that policy."

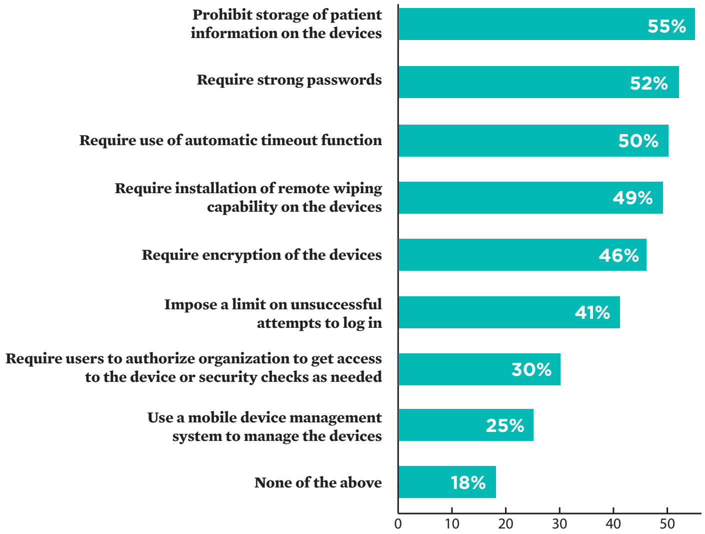
Does your organization allow physicians and/or other clinicians to use their personal mobile devices for work-related purposes?



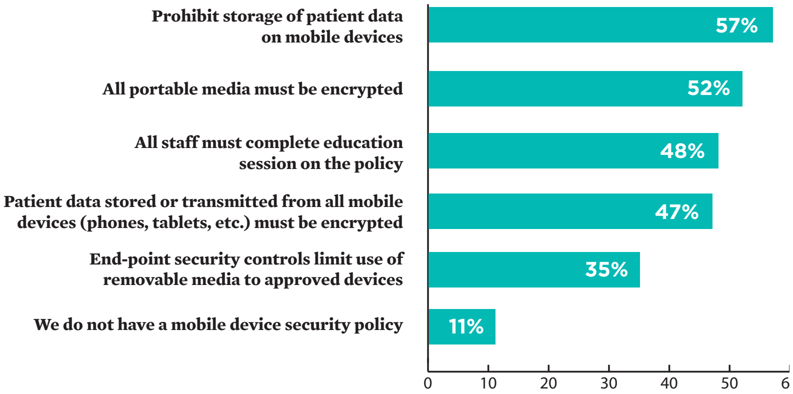
Regarding mobile devices, does your organization:



If your organization allows employees to use personally owned mobile devices for work, does your organization:

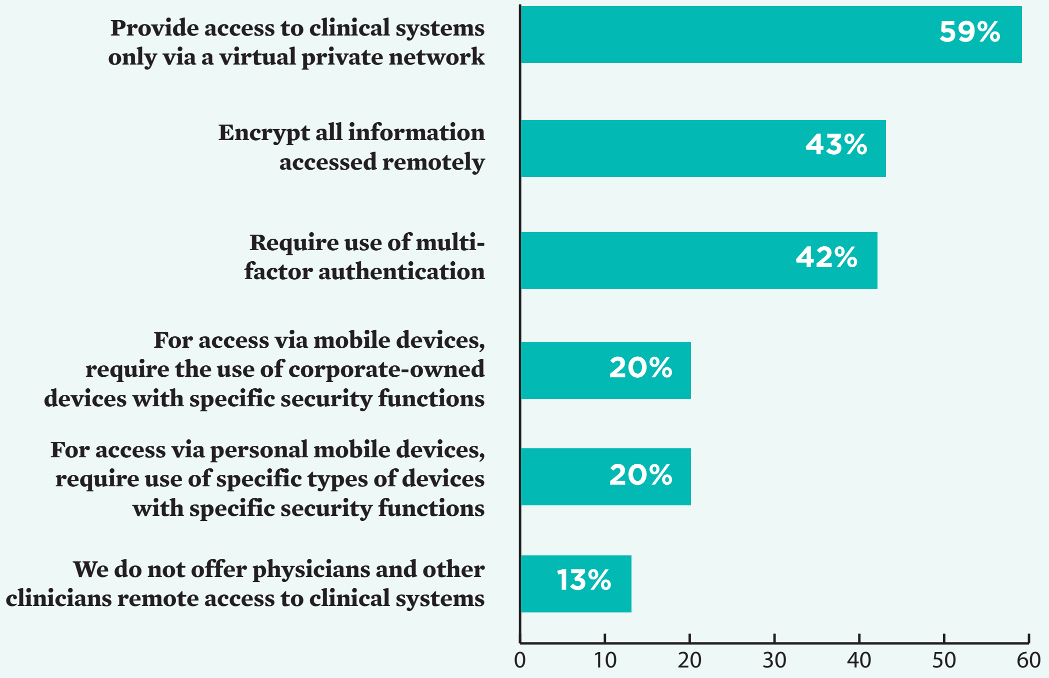


What are the major components of your organization's mobile device security policy?



Survey Spotlight: Remote Access

How does your organization address security for physicians and other clinicians who have remote access to clinical systems?



6. Cloud Computing: Concerns Persist

Many healthcare organizations are continuing to take a wait-and-see approach when it comes to cloud computing because of security concerns. The survey shows roughly two-thirds are not yet using cloud computing. The biggest reason why is concern about enforcing security policies and HIPAA compliance.

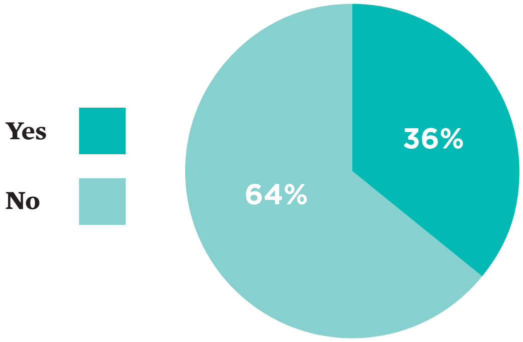
Of organizations that are using cloud computing, only 41 percent express confidence in the cloud vendors' access controls, and about half express confidence in the vendors' security policies and procedures. Clearly, cloud computing providers have a lot of work to do when it comes to winning the confidence of healthcare organizations.

Some healthcare CISOs complain that cloud services providers are reluctant to make available their security audit logs or penetration test results, which they see as essential to judging whether a vendor is trustworthy.

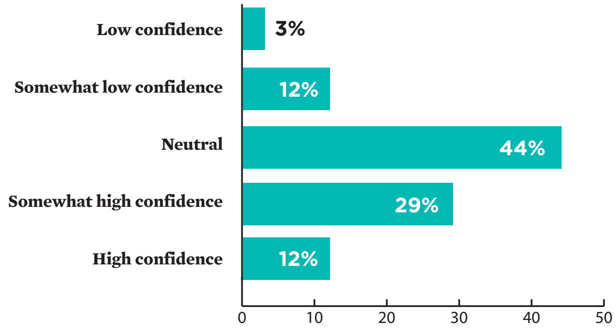
"The reality is that a lot of companies don't want to be transparent about their testing," says Jennings Aske, CISO and chief privacy officer at Partners Healthcare.

"Any software-as-a-service provider should have robust testing methodology and security testing that should be done by a third party," says Darren Lacey, CISO at Johns Hopkins University and its health system. "There should be full-on penetration testing, and the results should be made available to customers. But the problem is even those test results can be redacted."

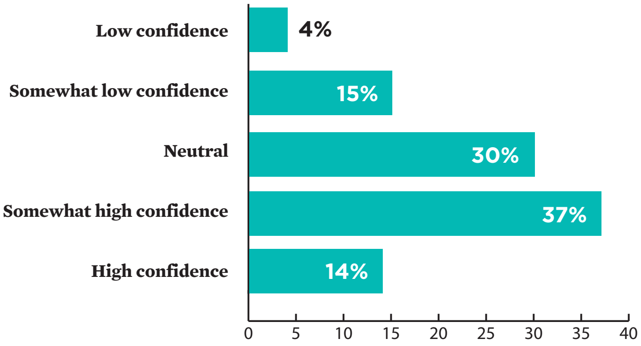
Does your organization use cloud computing, such as for remotely hosted applications or for data/image storage?



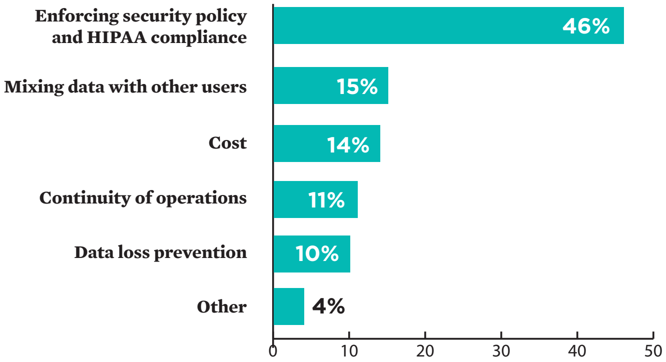
If your organization uses cloud computing, how confident are you in your access controls for cloud-based applications?



If your organization uses cloud computing, how confident are you in the vendor(s)' security policies and procedures?



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



The Agenda

In addition to complying with the new HIPAA Omnibus Rule, many organizations have plenty of other tasks on their information security to-do lists, the survey confirms. Here are some action items for 2013:

Improve Breach Detection, Prevention

In light of the thousands of breaches reported to federal authorities, healthcare organizations need to ramp up their efforts to prevent these incidents. They also need to improve their ability to promptly detect breaches and take appropriate resolution steps.

Closely Monitor Business Associates

Now that the HIPAA Omnibus Rule makes it crystal clear that business associates and their subcontractors must be HIPAA-compliant, healthcare organizations must take more steps to ensure their vendor partners with access to patient information are adequately protecting the data.

Ramp Up Training

Without adequate, ongoing privacy and security training, the risk of HIPAA violations and internal breaches remains unacceptably high. Organizations must go far beyond one-time training for new employees to make sure all staff members, and even volunteers, get frequent refreshers on how to help protect patient information.

Get Serious About Encryption, Authentication

Encryption and advanced authentication can play critical roles in preventing breaches. But many healthcare organizations have not yet made widespread use of these technologies. As part of their breach prevention efforts, hospitals, clinics and others need to carefully consider how best to apply these technologies as a way to mitigate critical risks.

Update Risk Assessments

The one-third of organizations that have not conducted a risk assessment in the past year will need to start updating their assessments annually to make sure all risks are adequately addressed. With the rapid adoption of mobile devices and other new technologies come new risks that must be mitigated.

Invest in New Technologies

The survey confirms growing interest in implementing mobile device management systems, which can play an important role in enforcing security policies. Other top planned investments include audit tool or log management systems and data loss prevention systems. Successfully implementing these and other new technologies will prove critical to protecting patient information.

Update, Enforce Mobile Security Policies

A majority of organizations allow clinicians to use personal mobile devices for work-related purposes. But mobile security policies are still evolving. Security leaders need to ensure that these policies are as up-to-date as the mobile technologies that staff members use. And that means spelling out requirements for personally owned devices.

Win Support for More Security Resources

Most healthcare organizations devote a relatively small portion of their IT budgets to data security. Increased funding is a good investment, given that it could help avoid breach-related costs that can quickly add up. But beyond more dollars, organizations need to ensure senior leadership creates a culture that values privacy and security.

Resources

Learn more about the key healthcare information security issues.

HHS Official Explains HIPAA Omnibus

Susan McAndrew of the HHS Office for Civil Rights offers an analysis of the rule, which extensively modifies HIPAA and provides new guidance about when to report a breach.

http://www.healthcareinfosecurity.com/interviews/hhs-official-explains-hipaa-omnibus-i-1772

Risk Assessments: Overcoming Inertia

Privacy and security experts, including Joy Pritts of the Office of the National Coordinator for Health IT, discuss the importance of frequent risk assessments.

http://www.healthcareinfosecurity.com/risk-assessments-overcoming-inertia-a-5289

How a Breach Led to Change In Culture

A breach that resulted in a $1 million HIPAA settlement led Partners Healthcare in Boston to take many significant steps, says CISO Jennings Aske.

http://www.databreachtoday.com/interviews/how-breach-led-to-change-in-culture-i-1738

Addressing BYOD in Healthcare

Organizations that allow staff to use personally owned mobile devices on the job need to develop a policy outlining the rules, says Kathryn Marchesini of the Office of the National Coordinator for Health IT.

http://www.healthcareinfosecurity.com/addressing-byod-in-healthcare-a-5455

Cloud Computing: Security a Hurdle

While cloud computing can provide benefits, two CISOs and a privacy advocate caution that security concerns are substantial.

http://www.healthcareinfosecurity.com/cloud-computing-security-hurdle-a-5404

When it comes to

We've got you covered.

News | Education | Research

BANKINFO SECURITY®
US | UK | EU | IN | Asia

CUINFO SECURITY®
Just for Credit Unions

GOVINFO SECURITY®

HEALTHCAREINFO SECURITY®

infoRisk® TODAY
US | UK | EU | IN | Asia

CAREERSINFO SECURITY®
US | UK | EU | IN | Asia

Data Breach® TODAY
Prevention. Response. Notification.
US | UK | EU | IN | Asia

iSMG
INFORMATION SECURITY
MEDIA GROUP

www.ismgcorp.com