2015

HEALTHCARE BREACH RESPONSE STUDY

INSIDE

- ***Complete Survey Results***
- ***Expert Analysis***
- ***Insights from Steve Claydon***,
  Professional Security Services Consultant, Solutionary

SOLUTIONARY®
AN NTT GROUP SECURITY COMPANY

ISMG
INFORMATION SECURITY
MEDIA GROUP

Tom Field

Breached entities Anthem, Premera Blue Cross and Community Health System make the big headlines, but healthcare organizations of all sizes are under heightened threat of breach.

How prepared are these organizations to respond to an attack, and what resources – in-house and outsourced – do they bring to bear to defend protected health information?

These are among the questions to be answered in the 2015 Healthcare Breach Response Study. In today's session, we will examine:

- **The state of breach preparedness at healthcare organizations;**
- **How entities are leveraging in-house resources, as well as managed security service providers;**
- **Top 2016 investments in technology, staff and MSSP.**

I will summarize the findings in the charts ahead, but generally what we discovered:

- **57% of respondents rate themselves above average or superior when it comes to detecting and responding to a breach, but ...**
- **54% have an in-house security team of only 1-5 people, and 23% still have no fulltime CISO.**
- **Respondents see their top threats in 2016 as unsecured business associates and mistakes by staff members.**

Join me in a review of the full survey responses, and then let's discuss how you can put this data to use to help improve your organization's capabilities to prepare for and respond to breaches.

Tom Field
Vice President, Editorial
Information Security Media Group
tfield@ismgcorp.com

About this survey:
This survey was conducted online during the summer of 2015, and we had roughly 250 respondents from US healthcare entities.

Table of Contents

Sponsored by

SOLUTIONARY®
AN NTT GROUP SECURITY COMPANY

Solutionary, an NTT Group Security Company (NYSE: NTT), is the next generation managed security services provider (MSSP), focused on delivering managed security services, professional security services and global threat intelligence. Comprehensive Solutionary security monitoring and security device management services protect traditional and virtual IT infrastructures, cloud environments and mobile data. Solutionary clients are able to optimize current security programs, make informed security decisions, achieve regulatory compliance and reduce costs. The patented, cloud-based ActiveGuard® service platform uses multiple detection technologies and advanced analytics to protect against advanced threats. The Solutionary Security Engineering Research Team (SERT) researches the global threat landscape, providing actionable threat intelligence, enhanced threat detection and mitigating controls. Experienced, certified Solutionary security experts act as an extension of clients' internal teams, providing industry-leading client service to global enterprise and mid-market clients in a wide range of industries, including financial services, health care, retail and government. Services are delivered 24/7 through multiple state-of-the-art Security Operations Centers (SOCs).

Big Numbers

Some stand-out figures from this survey.

53%

Rate as above average or superior their organizations' ability to manage privileged identities and external/internal access to critical systems.

96%

Say they are somewhat or very concerned about outside attackers compromising their corporate networks.

91%

Are somewhat or very concerned about legitimate employees, contractors or vendors abusing their privileged network access.

Baseline

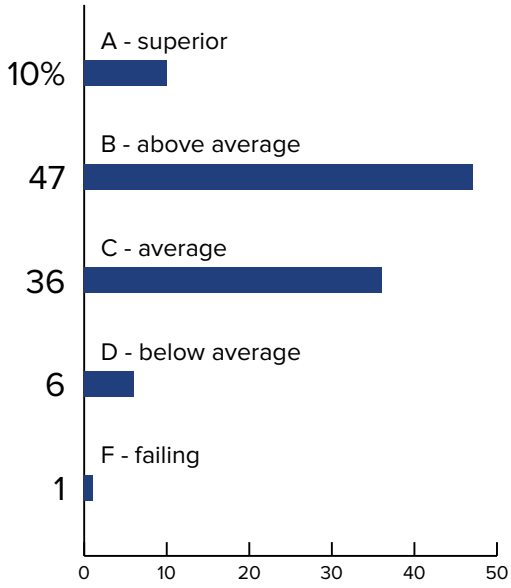
This first section helps establish a baseline for healthcare entities in terms of their abilities – perceived and in reality – to detect and respond to data breaches.

Among the standout statistics:

- **43 percent say breach detection/response capabilities are average or below**
- **Top nature of recent incidents:**
  - Misdirected fax or mailing
  - Insider attack
  - Malware infection

Next up: a full review of the responses in this survey segment.

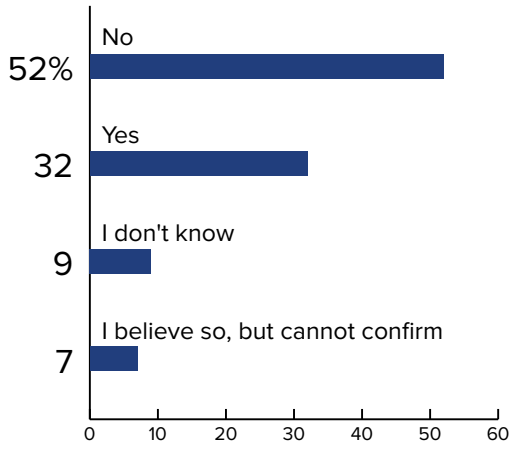
How do you assess your organization's ability to detect and respond to a breach of protected health information (PHI)?



On the surface, 57 percent of respondents generally feel good about their organizations' abilities to detect and respond to a breach, rating themselves at above average or even superior.

That confidence, though, is chipped away a bit when one asks more probing questions about recent incidents and their impacts.

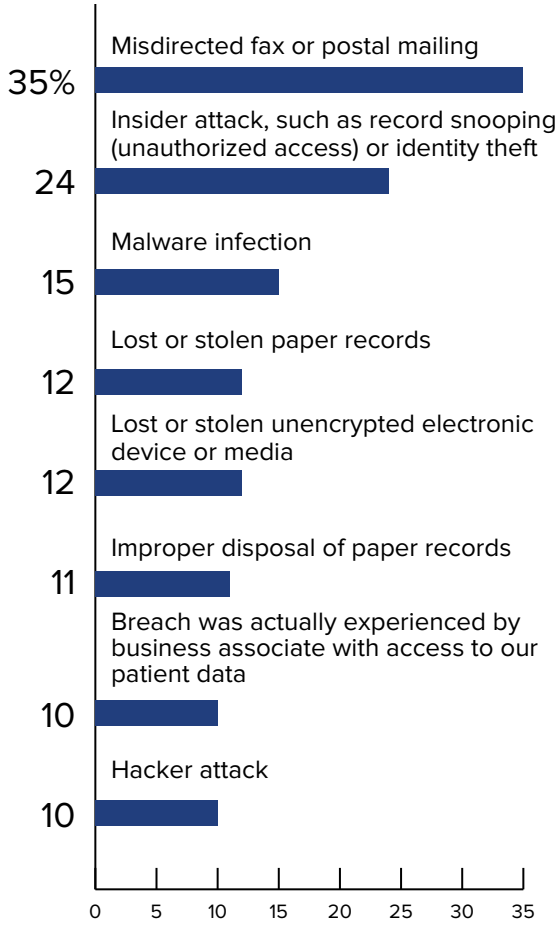
In the past 12 months, has your organization experienced a breach that resulted in the compromise of protected health information (PHI)?



In the past year alone, nearly half of respondents say they either have been breached, believe they were, or don't know (and "I don't know" often means "yes").

What types of incidents did they endure?

If your organization had a health data breach in the past 12 months, what was the nature of the incident(s)?



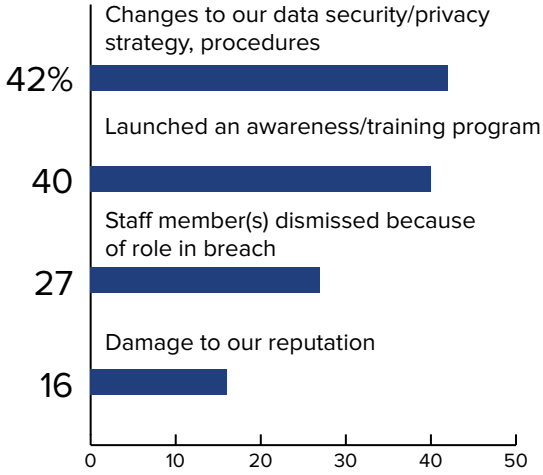
One can see the accidental nature of many of these incidents, as 35 percent of breaches result from misdirected mailing or faxes.

But these incidents are certainly not all so innocuous. Twenty-four percent of respondents report insider attacks (including medical record snooping), while 15 percent report malware infections.

Of special note here:

- **How few organizations report lost/stolen mobile devices, which to this point have been a leading cause of healthcare breaches;**
- **How few report breaches suffered by their third-party business associates – an area that federal regulators have paid great attention to in recent months.**

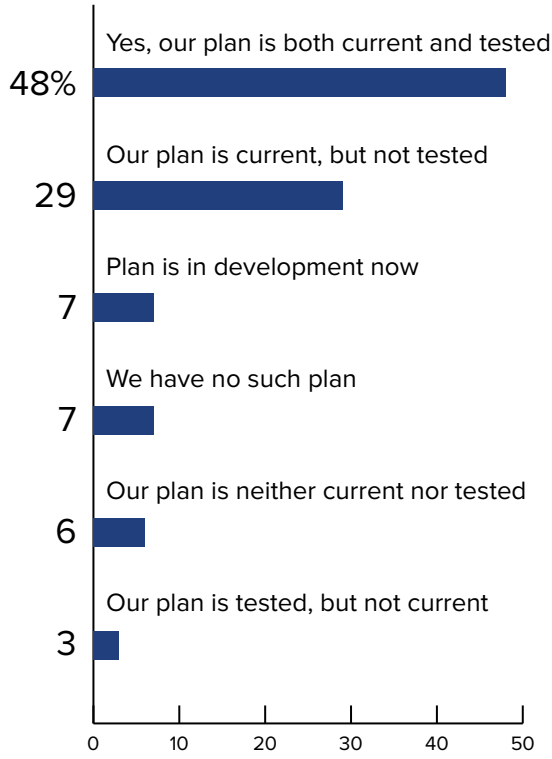
If your organization or a business associate had a breach in the past year, what was the impact?



What were the impacts of these incidents? Security policies and procedures were amended, awareness programs were strengthened or launched, and in some cases individuals lost their jobs.

Interestingly, despite all the publicity in healthcare about the federal “wall of shame,” few respondents cite reputational damage among their breach impacts.

Does your organization have a current and tested breach/incident response plan?



Here is where breach programs start to fall apart. It is hard to conceive that in this era of HIPAA compliance, federal audits and fines any healthcare entity would fail to have a current and tested breach response in place.

Yet, according to this survey, that is the case for more than half of the respondents.

The next section looks at the size and composition of the security team, which may offer some context for why important elements such as breach response planning lack sufficient attention.

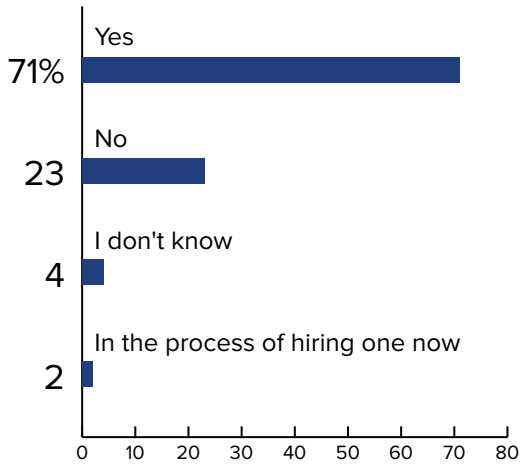
Security Team

Some important, upfront statistics about the current state of the security team:

- **29 percent of organizations have no CISO or equivalent**
- **42 percent rate in-house security expertise at average or below**

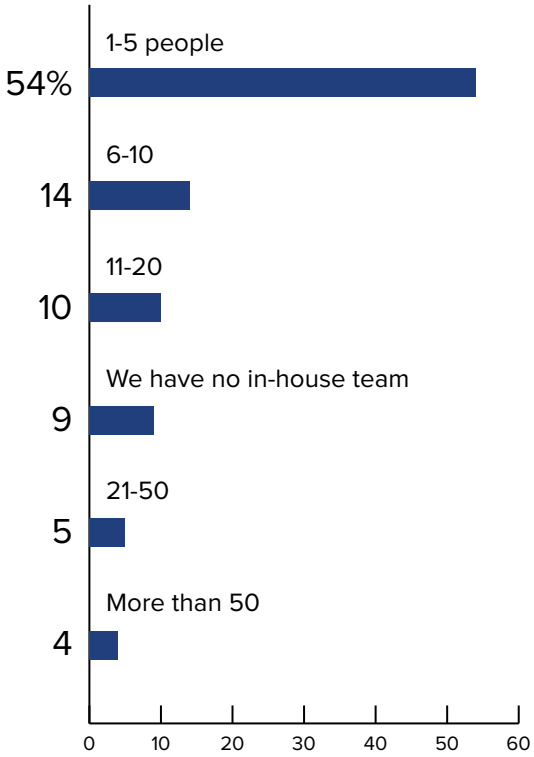
Full section results follow.

Does your organization have a full-time chief information security officer or an equivalent role?



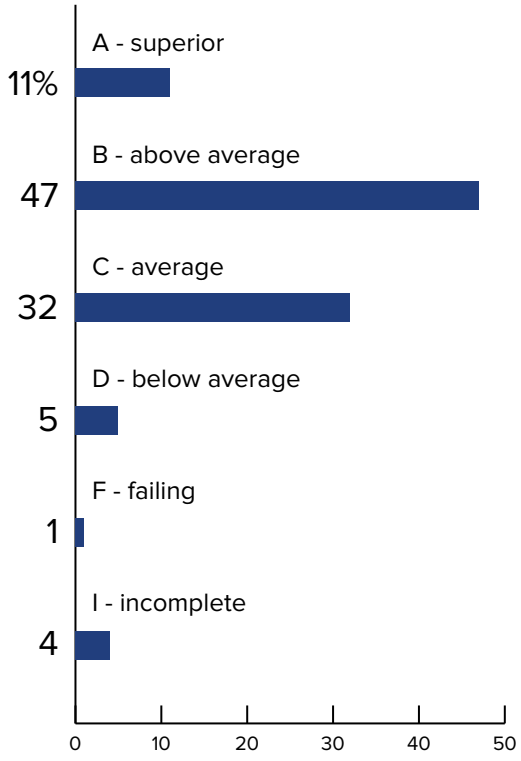
Encouraging to see that nearly three-quarters of respondents do have a CISO equivalent on the job. But seeing more than one-quarter who lack such a leader, it becomes easier to see why items such as response plans are lacking.

How large is your organization's in-house information security team?



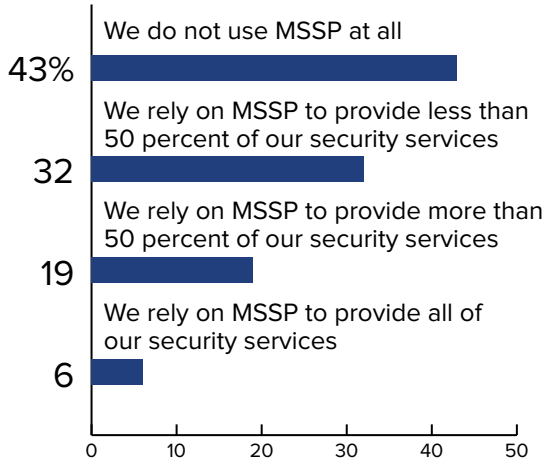
Consistent with research ISMG has done with financial services, healthcare information security teams are relatively small – under 10 individuals, for the most part. And nearly 10 percent have no security team at all.

How do you self-assess the level of expertise of your in-house information security team?



How do security leaders assess the general expertise of their in-house security teams? Not especially well. More than 40 percent offer a rating of average or less. And at a time when healthcare organizations especially are in the crosshairs for external attackers, "average" is hardly sufficient.

To what extent does your organization rely on managed security service providers (MSSP) to augment your in-house security team?



So, given the paucity of security professionals, as well as the lack of confidence in in-house skills, to what extent are healthcare entities leveraging help from third-party managed security service providers?

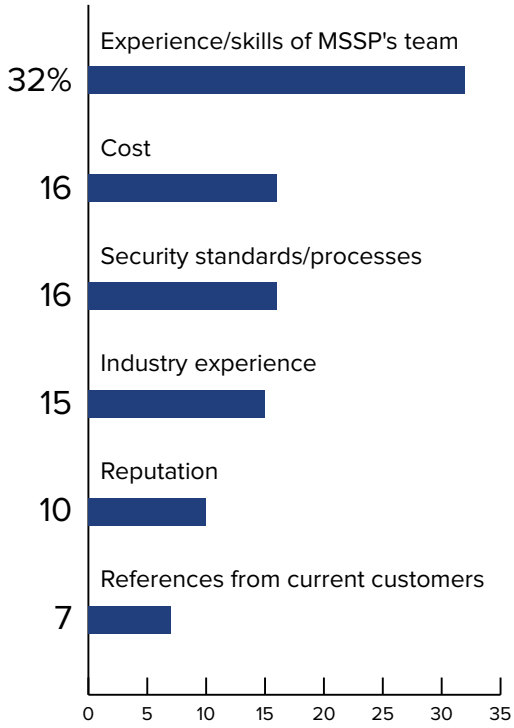
Fifty-seven percent use MSSP to some extent – including to provide all security services.

What are the most common outsourced services?

If you do currently engage an MSSP, which of the following healthcare security priorities do you entrust, at least in part, to these service providers?

The response runs the gamut, really, from general assurance of compliance to specific tasks that help ensure compliance, i.e. log management, health record encryption and developing a breach response/notification plan. Areas all that require deep and specific expertise.

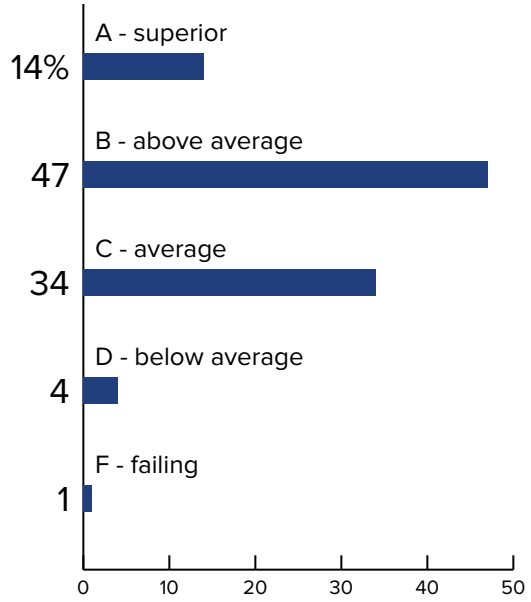
When it comes to selecting an MSSP, what factors are most important?



What do healthcare organizations look for when shopping for an MSSP?

Experience, primarily. They want a partner who understands healthcare, security and compliance – and that experience trumps other factors, such as cost and customer references.

If you currently employ an MSSP, how do you assess the vendor's current performance in protecting your organization from data breaches?



So for those organizations employing an MSSP, how do they assess the vendor's ability to protect them from breaches?

Better than they assess themselves.

Here you see that MSSP are graded above average or superior by 61 percent of respondents.

Next, a look at the 2016 security agenda and the role that MSSP will likely play.

2016 Agenda

When projecting 2016 investments, note these plans articulated by survey respondents:

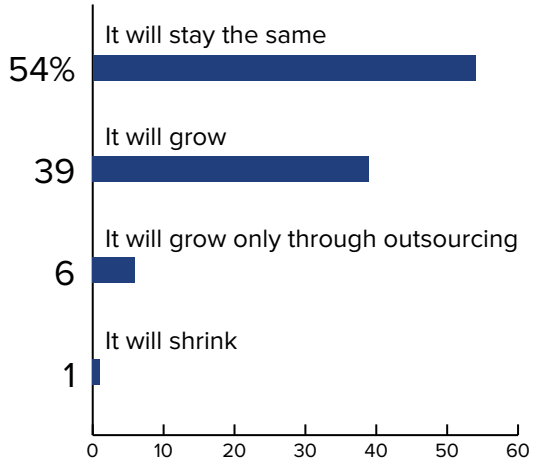
- **Top Threat: Business associates**
- **Technologies Targeted for Investment:**
  - Audit tool or log management
  - Data loss prevention
  - Intrusion detection, advanced malware detection, Multifactor authentication (tie)

In the coming year, what do you believe will be the single biggest security threat to your organization?

Despite that responding organizations to date have been more concerned about direct attack from outsiders and insiders, business associates are the main focus heading into 2016.

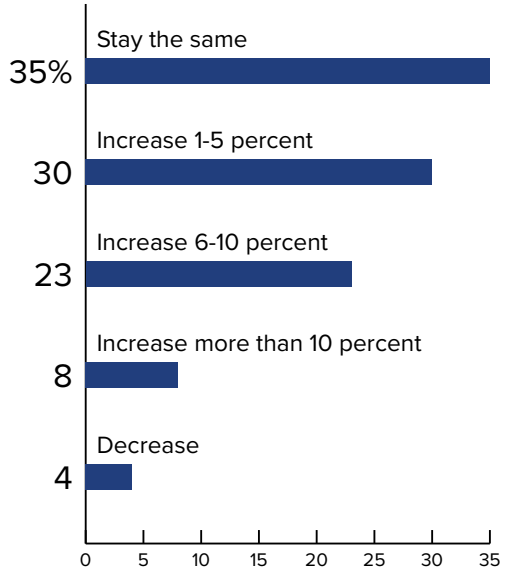
How will organizations staff up to address these concerns?

How do you expect your information security staffing to change in the coming year?



They won't. Fifty-five percent of respondents say the size of their security staff will either stay the same or shrink. Under 40 percent expect to hire additional in-house support.

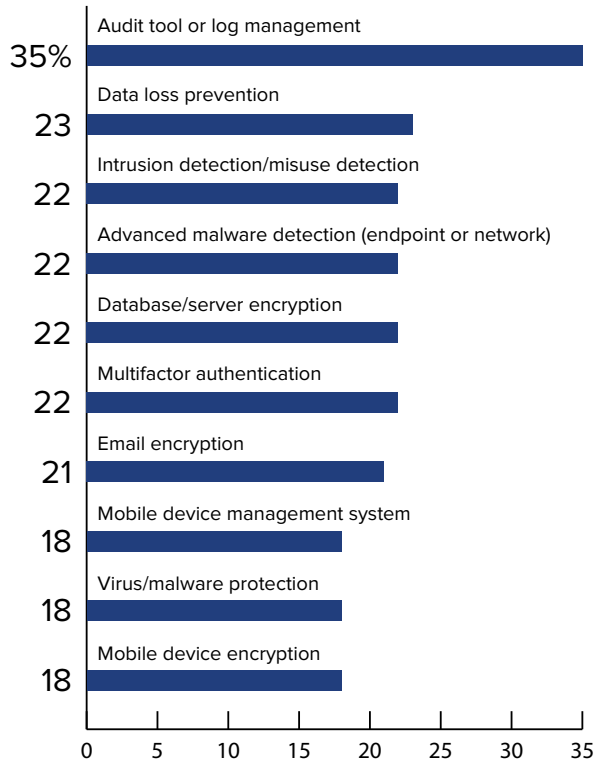
How do you expect your organization's information security budget to change in the coming year?



Very encouraging to see that 96 percent of organizations expect level-funded or increased security budgets in 2016, meaning there is room to augment the in-house security team.

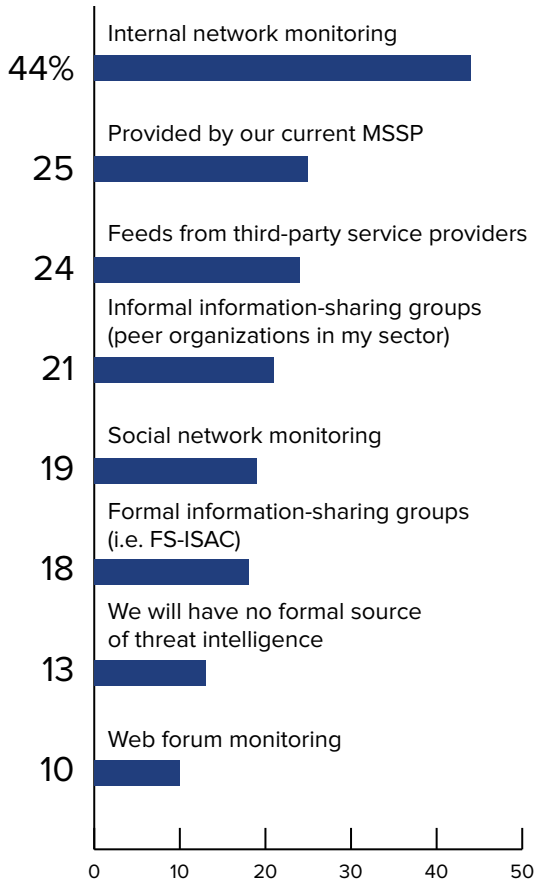
But if internal staffs are not growing, where will resources be directed?

Which of the following technologies does your organization plan to implement in the coming year?



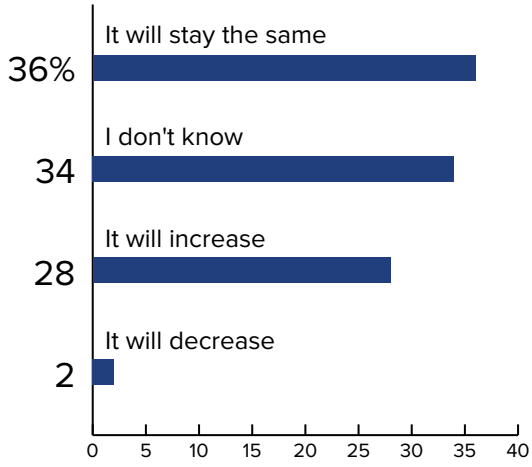
New technologies are part of the focus. Healthcare leaders intend to invest in new tools related to audit, data loss prevention, multifactor authentication and other security processes.

What will be your primary source(s) of threat intelligence in the coming year?



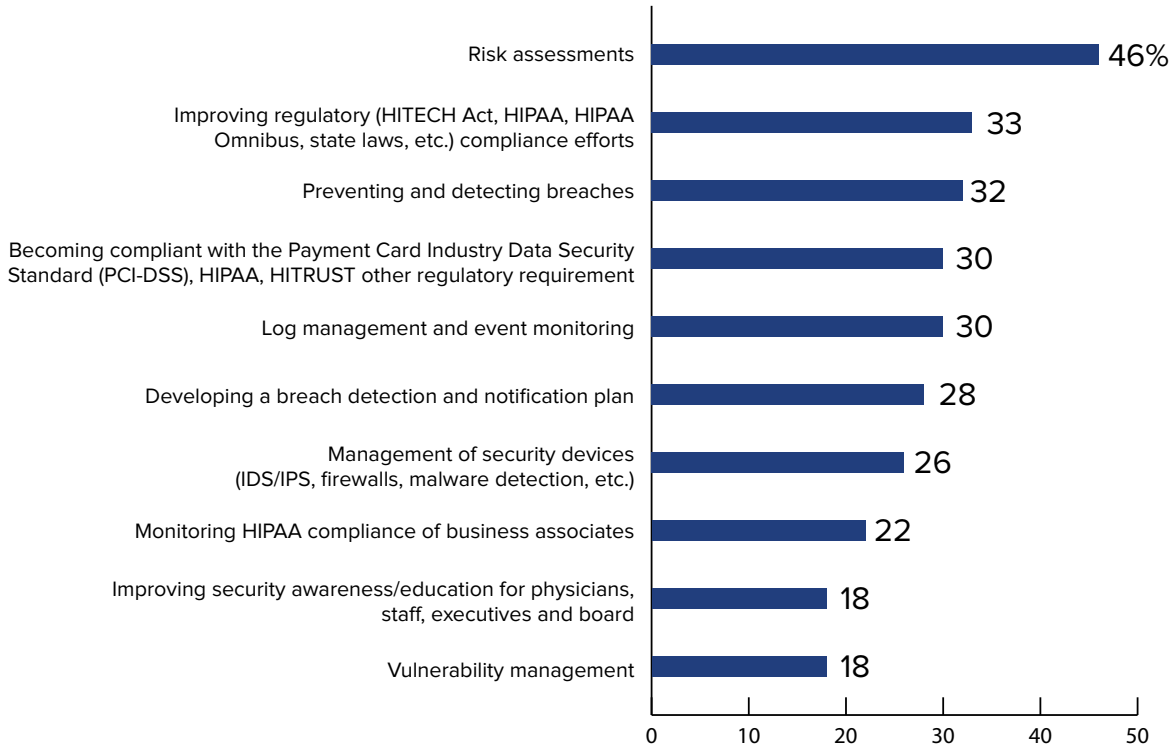
Threat intelligence is also a target, as security leaders expect to invest in new feeds and TI provided by MSSP.

How will your investment in MSSP change in the coming year?



But MSSP will also get a boost, with 64 percent of respondents saying they either will maintain or increase their current investment in these skilled third parties.

If you are planning to engage an MSSP/Professional Services in the coming year, which of the following would you entrust, at least in part, to a service provider?



Finally, for those organizations investing in MSSP, here is what they want: risk assessments, compliance and breach prevention.

In the next and final section focused on presenting survey results, see the conclusions from this initial analysis.

Conclusions

Some key conclusions to be drawn from survey results:

It's Not Just About BA's

Despite all the publicity and regulatory guidance about risks involving third-party business associates, security leaders are more concerned about critical systems being breached by external attackers and insiders.

In-House Skills Are Insufficient

Staffing is low; response plans are outdated/untested; leaders lack confidence in skills. These factors form a recipe for disaster. Organizations must enhance their in-house capabilities.

MSSP is a Growing Option

And if resources are not available in-house, then entities can look externally for professional services and managed security services providers. With outside help, organizations can: improve threat intelligence; gain access to needed skills; and leverage cutting-edge technology for security and compliance.

In the next section, Steve Claydon of survey sponsor Solutionary weighs in with analysis and some closing thoughts about how to put these survey results to work.

A Fresh Look at Breach Preparedness and Response

Survey Analysis by Steve Claydon of Solutionary

In preparation of this report, ISMG VP Tom Field sat down with Steve Claydon, Professional Security Services Consultant at Solutionary, to analyze the results and discuss how security leaders can put these findings to work in their organizations. Following is an excerpt of that conversation.

Claydon is responsible for developing and leading the healthcare security practice within Solutionary. Claydon's 20 years of experience in information technology, auditing, risk assessment and risk management along with his expertise in HIPAA security, privacy and breach requirements gives Solutionary clients an edge. Prior to joining Solutionary, he was Program Director at HITRUST where he was responsible for training programs and Common Security Framework kits. Claydon also led the creation of new programs that enabled HITRUST to continue to deliver leading-edge programs and tools to organizations responsible for protecting health information.

TOM FIELD: What's your first response to the results that we've talked about and what, if anything at all, surprises you?

STEVE CLAYDON: I think the one thing to me that did surprise me a little bit was the [lack of] BA preparedness. Healthcare has changed a little bit recently, and now business associates are required to meet all of the HIPAA requirements from a privacy and security perspective. So the onus is now on entities to audit and assess the BA's. I think it is interesting that they've not quite taken that piece on at the moment.

'What is Average?'

FIELD: Do you find that healthcare entities are maybe optimistic when they rate their state of preparedness at average or above, or do they maybe just have a poor understanding of what average really is?

CLAYDON: Maybe poor is not the right word, but I think they have a misunderstanding of what average is. I'm seeing today that average is almost like the new low, where organizations rate themselves as average, but in reality, when you go and you start doing some of these assessments, you find them a little below average and more on the low side.

I think there is a lot of optimism, but I also do think that the understanding of what security is required to meet a good level within the healthcare industry - it isn't quite what it needs to be. The finance industry, they're a little bit ahead of us at the moment, and we've got some catchup work to do.

"The understanding of what security is required to meet a good level within the healthcare industry - it isn't quite what it needs to be."

One of the things that always stands out to me is that if you ask someone, "Have you been attacked or have you been breached?" they'll say no. But then when you ask them, "Well, how do you know that?" They don't have a good answer. And I think we're seeing that as well in this whole business associates space as well. We're asking the questions, we're getting the answer back as no, and we're taking that as a good possible answer. I think we need to do more digging and do more of an assessment with those business associates, and that will give us better data as we move forward. I think that number that we're seeing today as small will be gradually increasing as we fix the problems, and then we'll drop back down again.

Steve Claydon

About Those Business Associates ...

FIELD: What's your take on the small number of incidents that our respondents attributed to third parties, given the focus that regulators have placed very specifically on this vulnerability?

CLAYDON: I think this comes back to organizations don't necessarily have a good handle on what they need to do and how to operate it. We're starting to see this in a number of areas. And I'm going to touch on some of this as we move forward as well. But VRM is really important in risk management - being able to manage your business associates. And I think the attraction to a small number of incidents is basically based on the fact that a lot of organizations aren't doing what they need to do. And they're not aware of what's going on at the business associate level. In addition, the business associates may not be reporting back correctly, as well. So if there's no data, we have no way of knowing how many instances are really occurring.

Lack of In-House Expertise

FIELD: Our respondents rate their in-house expertise as relatively low. When you look at organizations, where do you see the gaps in terms of expertise, and why aren't they being addressed?

CLAYDON: There are a number of factors I think that really drive this. And this is not just focused on healthcare; it's focused on the security industry as a whole. We're seeing a lack of skilled individuals. I mean, that's one of the things that the industry doesn't have today. It has a lot of people who claim they have good security knowledge, and there are lots of people out there that do, but there aren't enough skilled people to go around. So their in-house expertise is relatively low. We're getting people coming in, but they're junior in nature, and it takes a while. You can't pick up a couple of books and become a skilled expert. It takes a while for you to become seasoned and understand all the nuances of security.

The other area we see is that you do have some good skilled people, but they're pulled off of what they're doing and into commitments outside of security within the organization. So you're getting a network team saying, "Hey, can you help us look at this issue? Can you help us look at another issue?" And they're getting pulled away from their day-to-day work, which is truly the information security aspect.

And finally, one of the last things that we've seen - and this has been going on since even I started doing security - is the lack of true funding into the security enterprise. We always see it as a very, very small percentage of the overall information technology budget. So it's hard to get the right people. It's hard to keep them trained.

The Role of Threat Intelligence

FIELD: Let's talk about threat intelligence. What role should threat intelligence play in the security program for healthcare providers?

CLAYDON: It somewhat goes back to the previous question. If you lack that in-house skill set to do a lot of the work, then threat intelligence becomes probably one of the key pieces of the puzzle that you need to focus on. Threat intelligence obviously is going to allow you to look at the world outside and see what threats are coming in and give you some advance warning.

You can't rely on threat intelligence alone. A lot of threat intelligence services are very great and by their nature will provide you great information. But you still have to act on that information. And again, if you don't have those resources in-house to manage that information, you might be spending some money there and not getting full value.

Lack of a Response Plan

FIELD: I was stunned to see how many organizations don't have a breach response plan that's either current, tested or both. How can any organization get by today with a breach plan that's not both current and tested?

CLAYDON: It's an easy answer. You just can't do it. And it really doesn't matter how big or how small your organization is. The breach plan is, by its nature, so important a piece of information security, especially within the healthcare world. You've got regulatory issues to deal with if you don't have a breach plan in place. And I'm glad you touched on the point of current and tested. You know, I

> "You can't pick up a couple of books and become a skilled expert. It takes a while for you to become seasoned and understand all the nuances of security."

have a bunch of people who go out and do assessment work for the healthcare practice that I'm involved in, and they'll say to organizations, "Do you have a breach plan?" "Yeah, we certainly do," they'll come back to us. And we'll look at the document. It's dated five, six, seven years ago. And many things have changed within the organization. And it's not just technology. It's how you report, where you report, who you need to report to, the timeliness of all of these things. Without that breach plan that focuses truly on all aspects from the technology side to the reporting side, you are going to struggle. And the struggle is going to come in two forms: Your customers are going to have a lack of confidence with you. The data they've provided to you is secure, and if it does get breached, what is going to happen to that data, and what are the repercussions? And secondly, what are the fines that are going to take place with that?

So you've got a double whammy going on here. And organizations really need to take a look at that and spend a little time and focus on looking on what they have in place today. Does it take into consideration all of the things that they need to make sure for an application perspective, from a technology perspective, from getting the right individuals involved and from a reporting perspective? The simple and easy answer is you just cannot do it today without a good plan in place.

Top Risks to Watch in 2016

FIELD: As you take a look into 2016, what are the breach risks for healthcare organizations that concern you the most?

"Without that breach plan that focuses truly on all aspects from the technology side to the reporting side, you are going to struggle."

CLAYDON: Well, we touched on that right at the beginning when we talked about BA preparedness, and that's the one thing that really does scare me. We've seen lots of breaches recently, and a lot of them have been the insider attack or credentials going missing. But with HIPAA's requirements now, the BA's also are effectively covered entities and need to look after that information. Managing those business associates through some process is becoming increasingly important. You know, if you look at the standard organization in the healthcare industry, they don't do everything in-house. Billing and coding might go outside. Insurance claims are going outside. All of this information is being sent out to these business associates. But that's the bit that concerns me. Are we doing the due diligence on these business associates? And remember, most of them are legacy business associates. If you look up some of the big insurance companies, they've had these contracts in place for many years. So it's tough for them to go now and say, "Hey, I need to do this assessment on you, and it's going to cover a significant number of questions, and it's going to take a lot of time."

Now, the challenge you always have is: If Company A goes and does an assessment of a business associate, can they pass the results to someone else? Will they want to pass those results? So this business associate is getting hit with multiple requests constantly for information about their security within their organization. And this is where it worries me is: Are they really giving you their full level of effort and confidence that they're answering the questions correctly? We're seeing a lot of information being sent out of the company to the business associates, and if you ask the people that are sending it, it's "Where is it going? What type of data is being sent? Is it secure?" I think we're going to start seeing more and more the truthful answers of "We're not sure." And you're starting to see this with a lot of big insurance companies, where they are now mandating that their business associates start to go forth and do some level of testing to provide a level of assurance that the information sent to them is, in fact, secure.

Reduce the Risks

FIELD: So given the risks that we've talked about, how do you believe that healthcare entities can best manage and reduce their risks, and where do you see frameworks having a role in their risk reduction?

CLAYDON: Frameworks are a great, a great start. But I'm not a fan of checkbox security. What I do like organizations to do is to look at frameworks as the basis to their information security program. But it's not the be-all and end-all. So if you've gone through HIPAA security and you've gone and you've checked off all the boxes, yeah, you're meeting

all these requirements, but don't just stop there. Start to look at some of the other frameworks that might be able to complement you. Don't just focus on one.

And we see this not just in the healthcare industry. If you look at the finance/retail industry, a lot of those organizations, once they've done PCI, they feel great. They move on. I don't like that approach. What I like to use from a framework perspective is, "What is my priority frame? What is my main one?" You know, in healthcare, it's HIPAA. I've got to meet the security, privacy and breach laws. But then I should look outside of [HIPAA] and say, what else can I do to make more holistic security in my organization? So maybe I want to start looking at ISO and look at what that does. And it doesn't mean that you have to implement controls at such a granular level, but try and take that information and use it to enhance security in general.

I think it's my biggest issue, and one of my soapboxes is that we see a lot of organizations and companies perform checkbox security. That is not going to help you sleep at night. I would much rather go through a number of frameworks and look at how that impacts my business and do the things that make most sense for my line of business, what the business is trying to achieve than purely just checking off a number of boxes.

The Move to Managed Services

FIELD: Seems to me this makes a great argument for a managed security service providers. Where do you see the best opportunities in healthcare for MSSP?

CLAYDON: I look at when you're going out to choose someone with an MSSP, you need to look at it holistically. From a plan, a strategy perspective, it's very easy just to go out and engage someone. And you really want to focus on, first of all, what helps the business. Threat intelligence is another great area that an MSSP may or may not provide. But you want to look at it holistically. Look at it from a planning perspective. And then look at it from a strategy perspective.

> "We see a lot of organizations and companies perform checkbox security. That is not going to help you sleep at night."

But if I had to focus on a few things that your MSSP wants to do, first of all, perimeter management. Sounds really simple. Sounds really easy. And to be truthful, it is one of the bread-and-butter areas that MSSPs can do. But it is very critical. Your outside environment is where people are going to start to do their attacks. So perimeter security is very, very important. And with perimeter security, this is where we like to start to think about what else can you do from an offensive point of view? Let's start to use the MSSPs that have got good skills and use offensive security to determine how strong or how weak we are. And the important thing with that is to do it on a regular basis. So MSSP, in addition to managing your perimeter in a real-time basis, should also be probing as well at a regular time to see where vulnerabilities occur. Because at the end of the day, we have organizations who are changing their things inside their network. Maybe changing things in their perimeter, and the MSSP may not know a lot that's going on. Hopefully they do. But if they don't, that perimeter management, a regular offensive security check, is certainly going to be a great place to start with what they should do initially from that perspective. But planning and doing the strategy work is obviously critical.

Put Survey to Work

FIELD: How would you recommend that our audience use the results of this survey so they can really put these insights to work to benefit their organizations?

CLAYDON: I think organizations need to be very, very honest with themselves. And I do see that in the healthcare industry today. We work with a number of organizations that have said, "Look, we just want to get better. How can we do that? We realize we're not where we need to be." So focus on being honest with yourself. You always want to paint the best picture, but sometimes you have to pull up the rugs and look under the carpet, and you're going to find stuff you don't want to see. Be very honest because at the end of the day, you can go to management and say: "Look, this is the work that we've done. This is where we are. This is what we need to go forward." That's certainly going to start you off on the right foot.

So after you've looked to yourself and have been truly honest with what you

need to do, also look at the business needs. Where is your biggest risk today? Look at what the business is trying to achieve and focus on being an asset to the business. That's one of the things I also like to preach from a security perspective is, how can security be an asset? We don't want to be a hindrance. We want to work together with the organizations to get that going.

And finally, it's going to sound a little weird, but attain the achievable. Don't try and bite off more than you can chew. Look at the areas you've got gaps in today. Look at how you can fix them. But fix them smartly. Fix them with the right use of resources and costs so, you know, attain your achievable. Let's focus on small, easy items; attain the achievable and start to use the skill sets you have internally and that you can afford.

"How can security be an asset? We don't want to be a hindrance."

For more results and analysis from the 2015 Healthcare Breach Response Study, please see:
http://www.healthcareinfosecurity.com/webinars/2015-healthcare-breach-response-study-results-w-869

Want to learn more about breach response?

Check out these content resources.

How to Consume Threat Intelligence
Trying to consume threat data remains a difficult and highly manual process, says Solutionary's Joseph Blankenship. But better machine learning and artificial intelligence could make the task easier for enterprises.
http://www.healthcareinfosecurity.com/interviews/how-to-consume-threat-intelligence-i-2675

Maturity of Managed Services
As security threats evolve, so do the market and maturity of managed security services. Court Little of Solutionary discusses the new demand for managed services - and how organizations can get the most from them.
http://www.healthcareinfosecurity.com/maturity-managed-services-a-8133

2015 Healthcare Information Security Today Survey
Healthcare organizations must comply with federal HIPAA regulations to protect patient health data. But the ever-changing threat landscape requires more robust security risk management programs that can defend against the unknown. So how much progress are Healthcare entities making on regulatory compliance, and beyond that, their efforts to strengthen overall security and privacy of health data, including preventing and detecting breaches?
http://www.healthcareinfosecurity.com/handbooks/2015-healthcare-information-security-today-survey-h-60

RESULTS WEBINAR

2015 Healthcare Breach Response Study - The Results

Presented by Steve Claydon and Tom Field

Breached entities Anthem, Premera Blue Cross and Community Health System make the big headlines, but healthcare organizations of all sizes are under heightened threat of breach. How prepared are these organizations to respond to an attack, and what resources - in-house and outsourced - do they bring to bear to defend protected health information?

We launched this survey to determine:

- **The state of breach preparedness at healthcare organizations**
- **How entities are leveraging in-house resources, as well as managed security service providers**
- **Top 2016 investments in technology, staff and MSSP**

Join us to discuss the results.

REGISTER NOW: http://www.healthcareinfosecurity.com/webinars/2015-healthcare-breach-response-study-results-w-869

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

(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