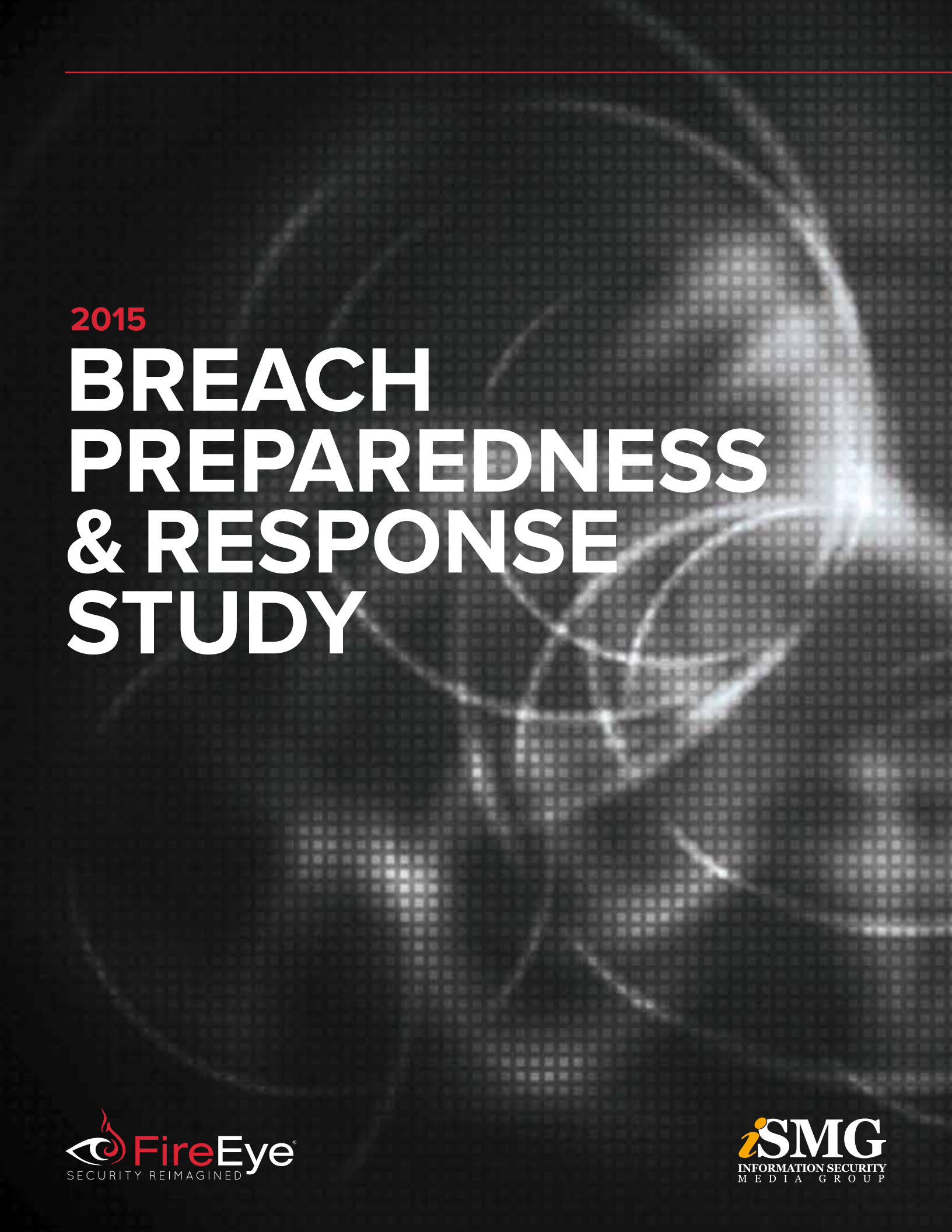

2015
BREACH PREPAREDNESS & RESPONSE STUDY
FireEye
SECURITY REIMAGINED
iSMG
INFORMATION SECURITY MEDIA GROUP

Tom Field

In 2013, ISMG and FireEye teamed up to survey security leaders about advanced threats and breach response. Among the findings: Only 20 percent of respondents rated their incident response programs "very effective," and they were most concerned about their abilities to detect and contain APT/malware quickly and completely.

Respondents also identified:

- **Top Threats** – Cybercrime and APT;
- **Biggest Gaps** – Effectiveness of current tools to detect and contain APT/malware;
- **2013 Priorities** – Data protection, training, automated tools.

Since then, we've seen a parade of high-profile breaches - including Target, Home Depot, Anthem, OPN, and Ashley Madison - that have only further exposed the vulnerabilities revealed in the 2013 study.

In 2015 ISMG and FireEye revisited information security leaders to gauge not just the deep impact of these breaches, but the state of global organizations to prepare for and respond to today's devastating cyber attacks.

The 2015 Breach Preparedness and Response Study is geared to determine just that: How well fortified are organizations to prepare for and respond to the inevitable? Are their security programs and controls truly as effective as security leaders believe them to be?

This survey was conducted online during the summer of 2015, and it drew more than 260 respondents from mid to large size organizations across multiple regions and industries.

We will dissect and analyze the key findings on the pages ahead, but to summarize: Organizations have made great strides in detection/response since 2013. But the threat-actors have made even bigger ones. It's time for security leaders to improve the quality of their threat intelligence, detection/response technology and the expertise of detection/response team – whether in-house or outsourced.

How do organizations intend to address these serious security gaps in 2016? Join me as we review the survey responses and – more important – discuss how you can put these survey results to improve your organization's ability to detect and respond to advanced attacks.

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

Table of Contents

Sponsored by

FireEye® SECURITY REIMAGINED

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time. FireEye has over 3,700 customers across 67 countries, including 675 of the Forbes Global 2000.

SURVEY ANALYSIS

Kevin Mandia on Threat Evolution

FireEye President on Today's Attacks, Attackers & Why Attribution Matters

The attacks have evolved, breaches have multiplied, and serious security gaps have been exposed. But what most concerns FireEye President Kevin Mandia? The rise of nation-states as leading threat actors.

In this excerpt of an exclusive interview, FireEye's president touches on several hot topics related to breach preparedness and response, including:

- Today's top threats and threat actors;
- Why attribution matters.

As President, Mandia oversees all operations since December 2013, when FireEye acquired his company, Mandiant. Before Mandiant, he was the Director of Computer Forensics at Foundstone (acquired by McAfee Corporation) from 2000 to 2003, and the Director of Information Security for Sytex (later acquired by Lockheed Martin) from 1998 to 2000. Kevin was also a United States Air Force Officer, where he was a computer security officer in the 7th Communications Group at the Pentagon, and a special agent in the Air Force Office of Special Investigations. He holds a B.S. in computer science from Lafayette College and a M.S. in forensic science from The George Washington University.

Threat Evolution

TOM FIELD: How is the cybersecurity landscape different today than it was two years ago?

KEVIN MANDIA: I think it's been a slow evolution. Having observed incidents for 20 years, I don't see the change and the rapid advancement everybody talks about. I see a more gradual change to where it's landed today, and that change has a lot of factors in it -- geopolitical condition, the efficacy of our defenses, how much data collection we have fully. I believe I'm in about the fourth stage of information security that I have looked at in the last two-and-a-half decades, and the biggest change is that there are just more sovereign nations where state-enabled hackers are active today, and the reason that's alarming is there's really no risk or repercussions to state-enabled or state-enacted intrusions.

When I say sovereign nation, obviously that does mean the capabilities or the boundary of the capabilities for the attackers is greater. I mean, they are going to get better because they have unfettered practice every day. They're operational every day. And while there's no risk or repercussions, obviously they up their game. There is nothing that makes anybody better than game time experience, and sovereign nations are gaining that on a daily basis. So, yes, ordinarily when there's an intrusion there is more discipline behind the intrusion, there's more advanced malware behind it, there's a better effort to be surreptitious and do counter forensics.

Need for Attribution

FIELD: If you were to offer a cybersecurity state of the union address, what would be a couple of your key points?

"There is nothing that makes anybody better than game time experience, and sovereign nations are gaining that on a daily basis."


Kevin Mandia

MANDIA: The first key point is attribution has to be right. There is no deterrent in cyberspace unless we know who did it. And, by the way, I believe the deterrent is largely outside of cyberspace right now. If you have a camera videotaping you, your activities are different. You behave differently. And right now in cyberspace, people are largely anonymous. The unfortunate reality of anonymity in cyberspace is a lot of times it accentuates the behaviors of bad people better than it safeguards the whistleblower types, so attribution has to be right. And I think as more and more critical components of our lives depend on the authenticity and quality of the data that's on the Internet, we're going to want to make sure people who do computer intrusions and break certain laws are held accountable.

Top Threats

FIELD: What are the security threats that concern you the most today?

MANDIA: Without a doubt, the thing that concerns me the most is just the authenticity and genuineness of data on the Internet. Let me give you an example: Ashley Madison [the adulterer's dating site] is compromised. That's a terrible thing in and of itself, both for Ashley Madison and for their customers. But who's to say during an election year that whoever did the intrusion didn't add a few names [to the leaked client list]? Why not? There's no way to tell the integrity and authenticity of that data, and yet that data being posted, whether genuine or not, can ruin lives, ruin families, ruin aspirations, and so that to me is the next frontier.

I just noticed an article just yesterday or the day before the head of the NSA was saying the same thing. I've had this concern for awhile. If we get attribution right, people will think long and hard before they lie, fib, cheat and steal. But I'm not convinced we're getting attribution right all the time. And second, when intrusions are happening and the data can't be trusted, both the data that remains, as well as the data that is publicly shaming people, that becomes a great issue. That's a problem. So I think that's the next frontier; the hackers that break in and make stuff up.

To hear the entire interview with Kevin Mandia, visit: http://www.inforisktoday.com/interviews/kevin-mandia-on-state-cybersecurity-i-2903

Big Numbers

Some stand-out figures from this survey.

51%

Do not have a breach response plan that's been updated and tested in past year.

56%

Rate the value of their current threat intelligence at average or below.

67%

Rate as average or below the maturity of their in-house breach response skills in comparison to those of threat-actors targeting their organizations.

I. Baseline Defense

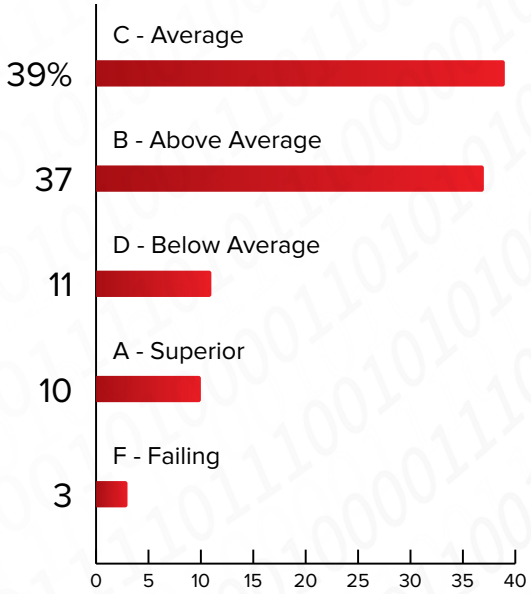
In this opening section, the questions are geared toward taking the pulse of the respondent community: What is their general assessment of their breach preparedness and response capabilities, and how frequently do they believe their organizations are targeted by threat-actors?

Among the findings:

- Only 47 percent rate their ability to detect/respond at above average or superior
- 61 percent know they have been targeted by threat-actors in the past year

Complete "Baseline" results follow.

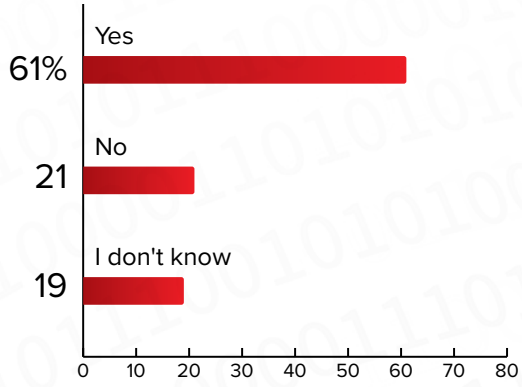
How would you rate your organization's ability to quickly detect and respond to targeted attacks before they result in significant business impact and/or data theft?



On the surface, respondents generally feel good about their organization's defensive posture, with 47 percent rating themselves above average or superior when it comes to detecting and responding to targeted attacks.

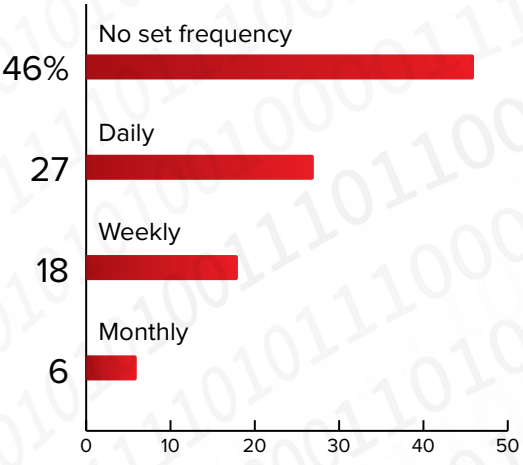
It is only when the questions probe deeper that respondents start to reveal vulnerabilities that cast doubts on these capabilities.

In the past year, has your organization been targeted by threat-actors trying to get into your network and gain access to protected data?



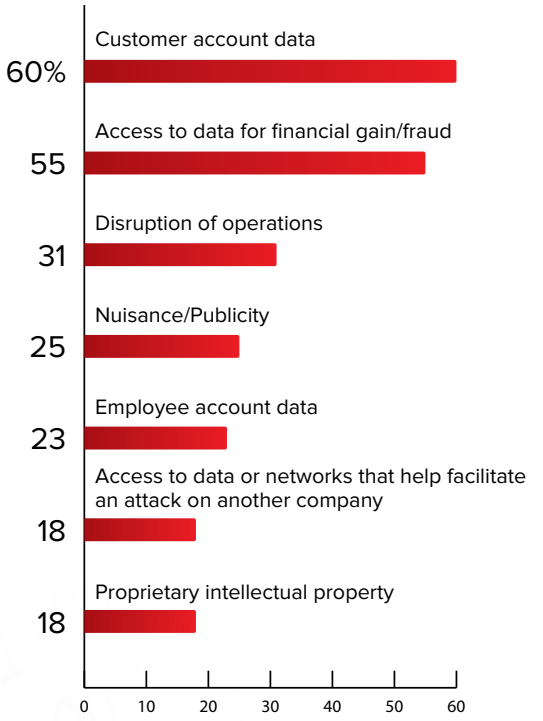
The key figure here is not the 61 percent that know they have been targeted over the past year – nor even the one-fifth who say they have not. Instead, take note of the 21 percent who say "I don't know." In an age when advanced threats can go undetected within organizations for months – and given later survey responses that reveal some challenges in detecting attacks – it is likely that many of these "I don't know" organizations indeed have been targeted.

If you answered yes to the previous question, what is the frequency of targeted attacks on your network over the past year?



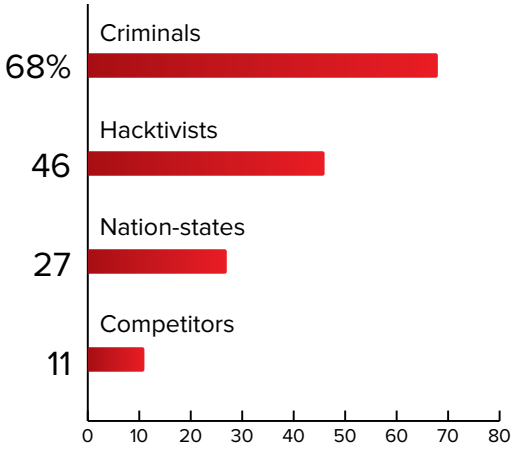
It's just a part of daily business now. More than one-quarter of organizations say they are targeted on at least a daily basis, but nearly half say there is no set frequency. This puts the onus on security staff and controls to maintain constant vigilance.

If you answered yes to question 2, what do you believe to be the threat-actor's main motives for attacking your network?



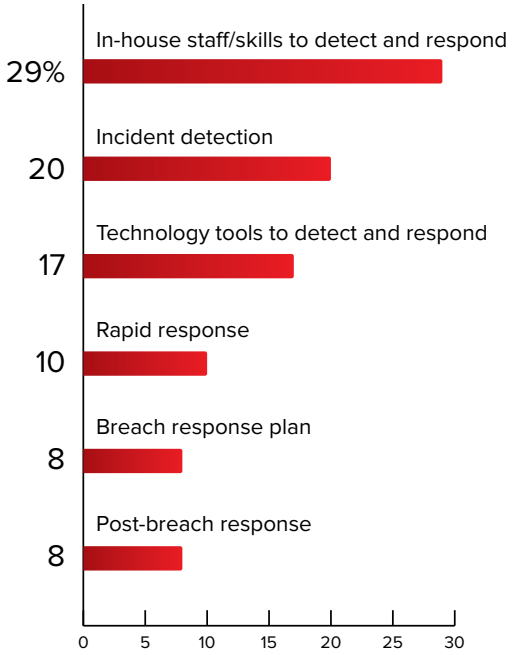
Interesting to see "financial gain/fraud" in second place on this list. The ranking reflects changes in the breach landscape, where the latest high-profile hacks – OPM and Ashley Madison stand out – do not appear to have been launched by attackers seeking financial gain by, say, cashing out on payment card information. Rather, the goal is to procure customer account data, which can be used for nefarious purposes that range from committing identity fraud to potentially attempting to blackmail account holders.

Whom do you believe to be the threat-actors most interested in penetrating your network?



The nation-states get the headlines – i.e. Korea being blamed for the Sony hack, and China being pinned for the OPM breach and others. But respondents say they most frequently are targeted by criminal groups (68 percent), and hacktivist organizations are prominent, too (46%). The nation-states place third at 27 percent.

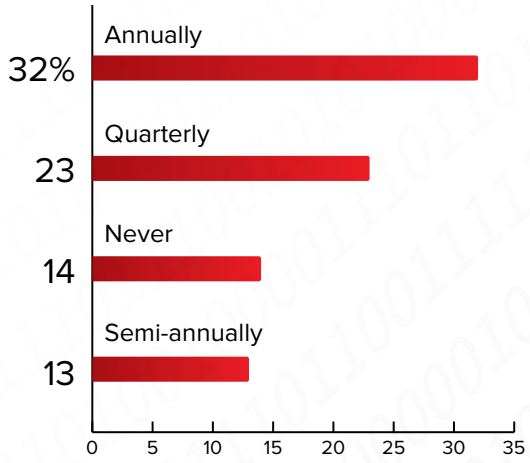
What do you believe to be your organization's single weakest area of breach preparedness and response?



It isn't about the plan; it isn't about the tools. Rather, the single biggest weakness when it comes to organizations' abilities to prepare for and respond to breaches ... is people. Nearly one-third of respondents cite their in-house staff and skills as their greatest vulnerability.

Later in the survey, questions will probe deeper into which specific skills are lacking – and how organizations plan to address the deficit.

Has your organization conducted an assessment to determine if your network is compromised? If so, how frequently do you conduct such assessments?



Given that nearly one-fourth of organizations said earlier that they are targeted on a daily basis, it seems to be a disconnect that 32 percent of respondents conduct compromise assessments only annually.

But, then, most regulatory standards recommend annual assessments as their own baseline minimums. It is encouraging that nearly one-quarter of respondents conduct quarterly assessments, but unfathomable that 14 percent claim "never."

The next section of the report will explore the topic of breach preparedness in depth.

FOCUS ON DETECTION

How Quick Do We Spot Attacks?

Survey Analysis by FireEye CTO Grady Summers

Q: So, in your experience, how good are organizations at 1) knowing they've been targeted by threat actors and 2) detecting those attacks somewhere near real-time?

Grady Summers

GRADY SUMMERS: That's an area where we have done a lot of empirical research going back about five years or so. Mandiant has a M-Trends report where we track how long attackers were on victim networks and who is discovering breaches.

As we go back four or five years, organizations were finding attacker activity, and the median number of days was 412 days. Remarkably long. But things have improved a lot. In 2014, the median amount of time that an attacker was on the victim network was 205 days. So you can see two things: a great deal of improvement, but also that's an awfully big number, so I think we've got a long way to go.

We also track how organizations discover breaches, and back in 2012, only 5 percent of the companies found breaches on their own. Last year, that increased to one-third of organizations finding breaches on their own.

But that still means two-thirds of them are not, so I kind of look at it as it's glass half-full, glass half-empty. There's been an awful lot of improvement, but I think we can say pretty easily that if only one-third of organizations are finding their breaches on their own, and the median amount of time is still 205 days, we're still not doing really well.

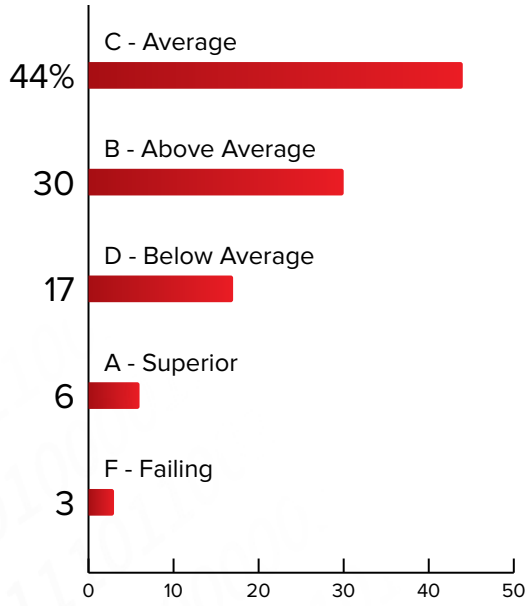
II. Breach Preparedness

And here is where the survey starts to dig below the "feels good" surface of the earlier responses. Among the key findings about breach preparedness:

- Only 49 percent have an updated, tested response plan
- 56 percent rate the value of their current threat intelligence average or below

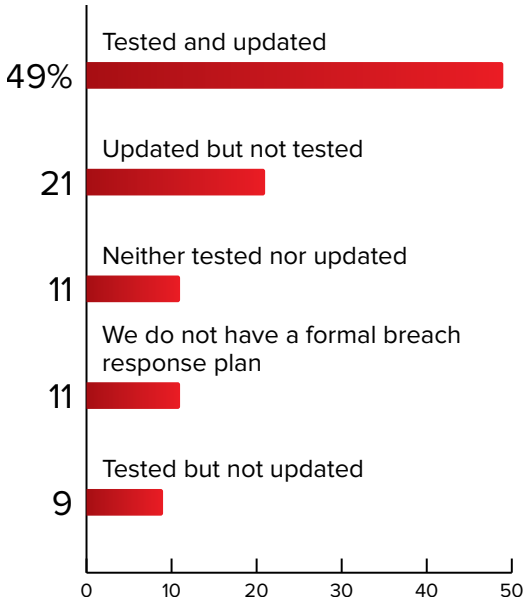
Detailed results are on the following pages.

How would you rate your organization's current state of breach preparedness in relation to the skills and persistence of today's threat-actors?



In security, there is an adage that "Organizations need to be right 100 percent of the time; attackers only need to be right once." Given that reality, it is disconcerting that nearly half of respondents rate their state of preparedness as "average" in comparison to the skills and persistence of their adversaries.

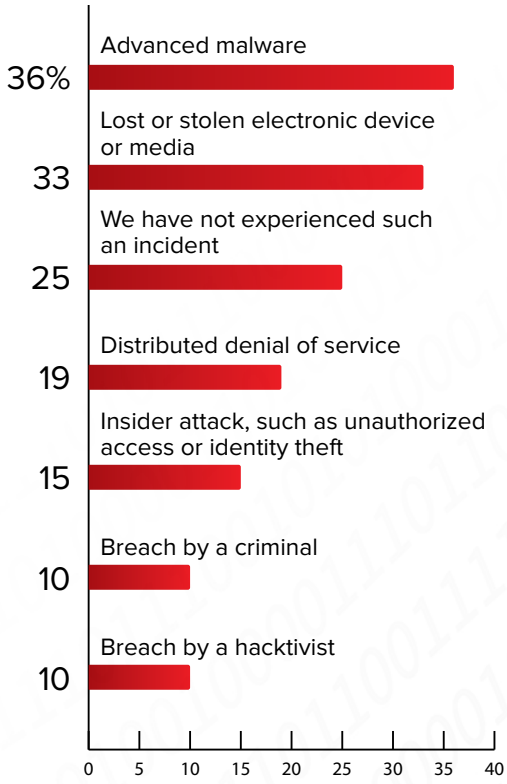
Has your organization's breach response plan been tested or updated in the past year?



Given the proliferation of high-profile breaches, it is surprising to see that fewer than half of respondent organizations have breach response plans that are both current and tested.

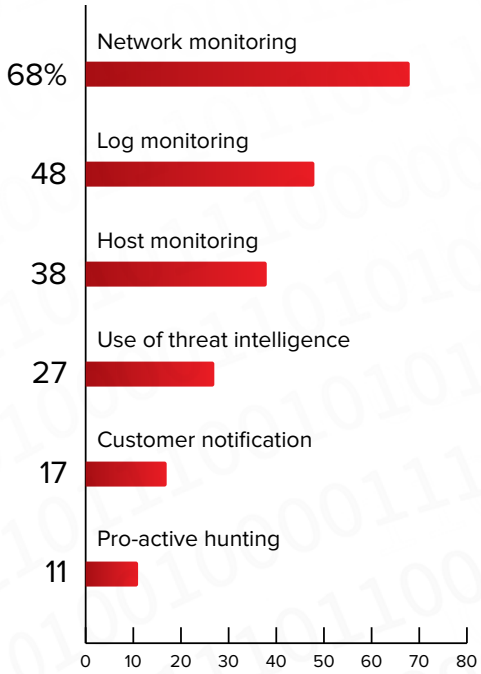
Even more stunning: More than 10 percent still lack formal plans.

What type of security incident or network breach has your organization experienced in the past year?



True to trends evidenced in recent breaches, the highest number of respondents (36 percent) report advanced malware – the foundation of advanced persistent threats – as being the key ingredient of their own security incidents in the past year. Second on the list: Lost or stolen devices or media, which account for one-third of incidents.

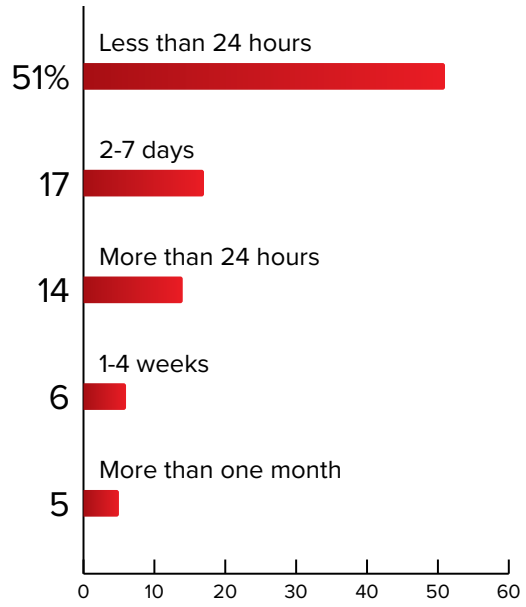
What was the most effective means for detecting the incident(s)?



When it comes to detection, respondents indicate that their tools are working. The top means of detecting incidents are network monitoring, host monitoring and log monitoring.

The number that one wants to keep low is this: the percentage of incidents that organizations learn about only when notified by their customers.

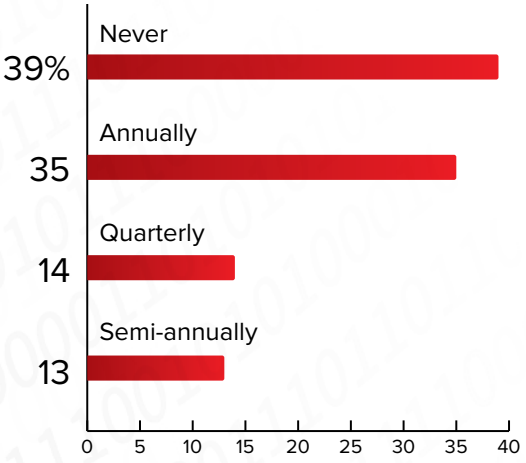
On average, how long did/does it typically take for these incidents to be detected?



More than half of organizations say they typically can detect these incidents in less than one day. This is an encouraging finding, given recent industry reports that say advanced threats can go undetected for 200 days or more.

Later in the survey, the detection rates will be compared to response times – which are less encouraging.

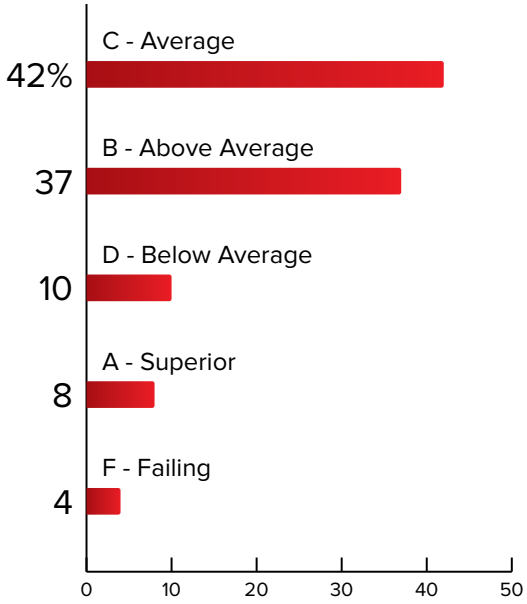
Has your organization conducted an assessment simulating an attack by a targeted threat actor to determine the effectiveness of your detection tools/processes? If so, how frequently do you conduct such assessments?



So-called tabletop exercises are less common than breach response experts would recommend. Only 35 percent of respondents say they conduct these annually, while nearly 40 percent say they never perform such tests.

Yet, without simulated attack exercises, it is challenging to know how effective breach response plans and teams may be when the incident is real.

How would you rate the value of the threat intelligence your organization currently receives?

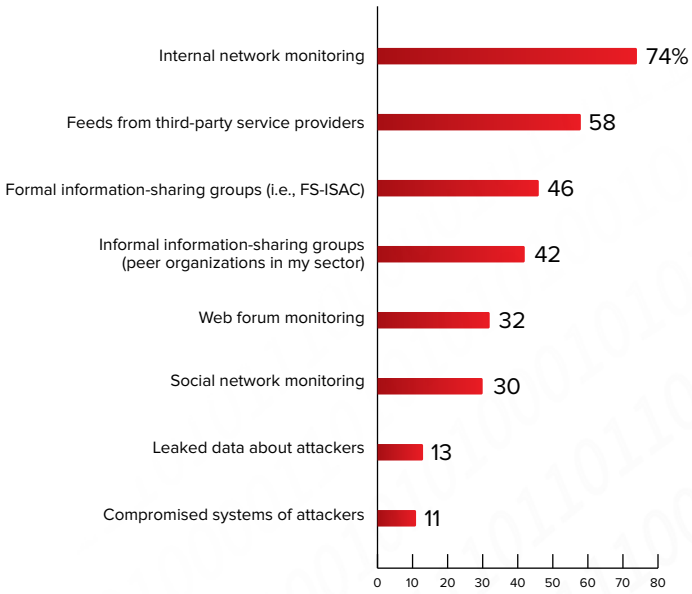


"Threat intelligence" is one of the hottest cybersecurity buzz-terms. Everyone seemingly puts a premium on it and wants to see more of it shared across industry. In theory.

But in practice, more than 50 percent of survey respondents rate their current threat intelligence as average or below. Only 8 percent rate it as superior.

What are the current sources of TI, and why are they rated so poorly?

What are your organization's current sources of threat intelligence?



The bulk of current threat intelligence comes from internal network monitoring, with feeds from third-party service providers placing second. Third on the list is TI from formal information-sharing groups such as FS-ISAC in the U.S.

This topic will be discussed prominently in the survey analysis, later in the report. But next the results will transition from breach preparedness to response.

FOCUS ON PREPAREDNESS

Tapping the Value of Threat Intelligence

Survey Analysis by FireEye CTO Grady Summers

Q: The majority of respondents don't rate the value of their current threat intelligence particularly high. Why do you feel that is?

Grady Summers

GRADY SUMMERS: That's consistent with what we would see, as threat intelligence operations are still fairly nascent. Threat intelligence is something that organizations know that they want, but they don't know quite how to develop it internally. And we still find that organizations don't quite know what to do with the threat intelligence when they get it.

And I think it goes back to a statistic I mentioned earlier, which is that only one-third of organizations are discovering breaches themselves. That tells you right there that orgs don't necessarily know what to look for, they're not applying threat intelligence in the right way.

But I would make a couple of other comments here. One is that developing a threat intelligence operation is extremely hard. We find that the resources are very hard to come by. They're not the cheapest resources either, and there is just, honestly, a limited supply of analysts who know how to properly service and discover threat intelligence, process it and put it in context. Organizations who want to do well here - even if they've got an in-house team - they're heavily supplementing it with third-party organizations that can provide intel. But again, the orgs that do this well have thought about 'what am I going to do with this threat intel when I get it? How am I going to apply it? How am I going to use both the indicators and the more discreet technical aspects of that intel, as well as the more contextual, strategic piece of the intel?'

I think one of the worst things an org can do is just subscribe to a threat intel feed without a good plan of what to do with that threat intel.

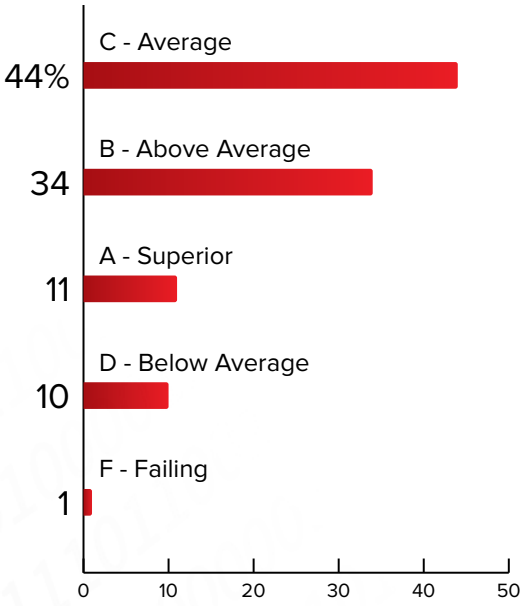
III. Breach Response

This section reveals the gulf between breach detection and response. Among the key findings:

- 45% rate their organizations' response capabilities at above average or superior, but ...
- 61% say it takes from one day to over one month to resolve incidents

Full breach response results are revealed in the next several charts.

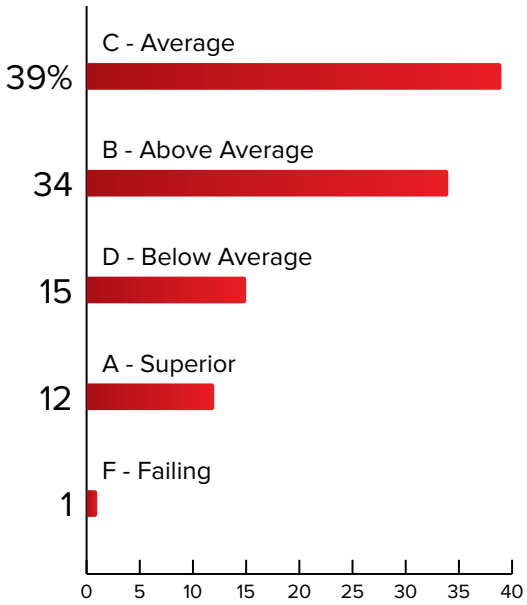
Once a breach is detected, how would you rate your organization's ability to investigate and respond effectively?



Again, when asked a "how do you feel" question, respondents rate their investigation/response capabilities fairly well. Forty-five percent say there are above average or superior.

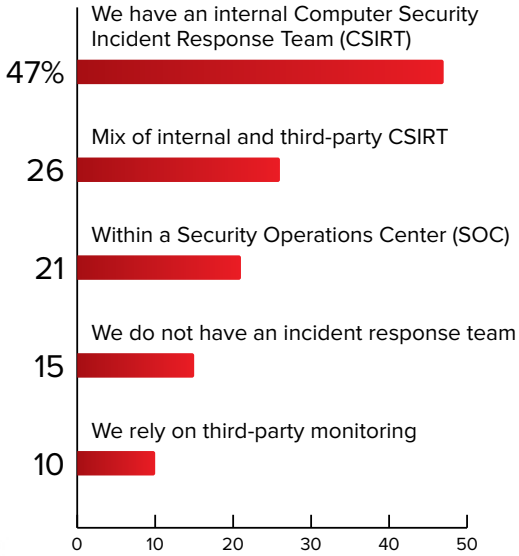
But 44 percent rate themselves as average, which is a tough stance to take against advanced, persistent adversaries.

How would you rate your organization's ability to determine the entry point of a threat actor and the extent of their infiltration into your network?



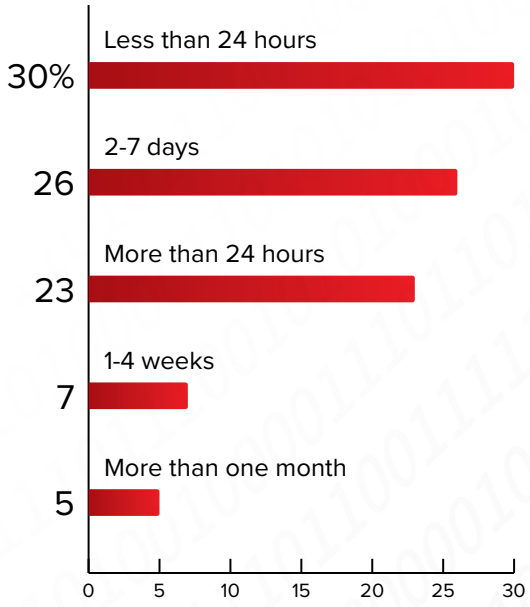
When it comes to determining entry points of intrusions, as well as the extent of the infiltration, a majority of respondents rate themselves either average or above. Another point in favor of detection capabilities.

How is your incident response team organized?



Breach response has been formalized in many organizations. Nearly 50 percent say they have an internal computer security incident response team, while more than one-quarter have a mix of internal and third-party CSIRT.

Following breach detection, what is your organization's mean time to resolution (MTTR)? (include both remediation steps such as eradication or containment as well as recovery to normal operations)



And here is where the gap between detection and response manifests. In contrast to the majority of respondents that say they can detect an incident in less than 24 hours, here 61 percent say it takes them anywhere from one day to more than once month to resolve such incidents – including eradication, containment and recovery to normal operations.

With such a long, ranging response time, the opportunity for significant business compromise is huge.

Why such a gulf?

What do you believe are the top 3 technical and/or organizational challenges that impact the ability for effective incident response?

It comes back to people once again. When asked to list their top three challenges to effective incident response, organizations start with a lack of skills and personnel to investigate and contain the breach.

But people are hardly the only vulnerability. Placing a very close second on the list is a lack of tools to quickly investigate and contain.

The next section explores exactly which tools organizations currently deploy.

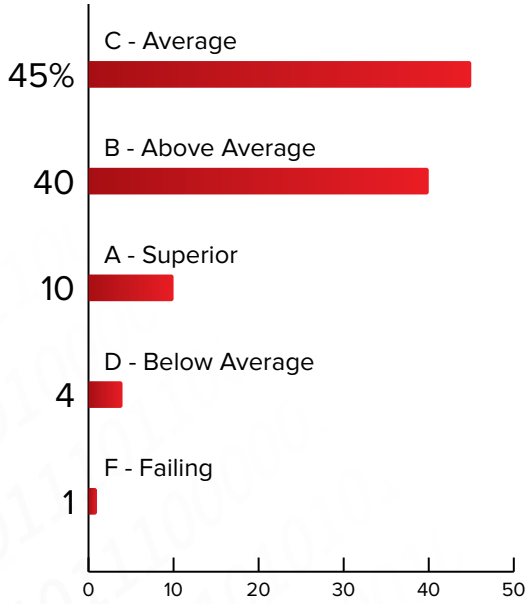
IV. Tools & Skills

If there has been any single, consistent lesson from this age of advanced threats, it is this: Traditional security tools are insufficient to detect and respond to nontraditional adversaries. Survey results support this statement, with respondents saying:

- 50 percent rate their current anti-malware tools at average or below
- 47 percent say their biggest skills gap is forensics investigations

Full results and analysis follow.

How would you rate the effectiveness of your current anti-malware tools?

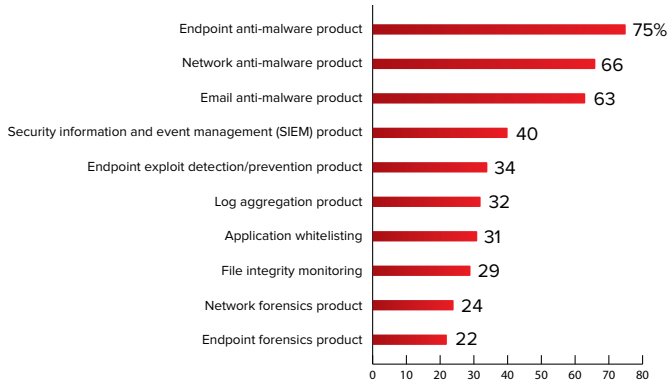


There is a current market debate about “Is AV dead?” And while this survey report will not settle the question, it does add points for consideration.

Only 50 percent of respondents say their current anti-malware tools are above average or superior. Just as many say they are average or below.

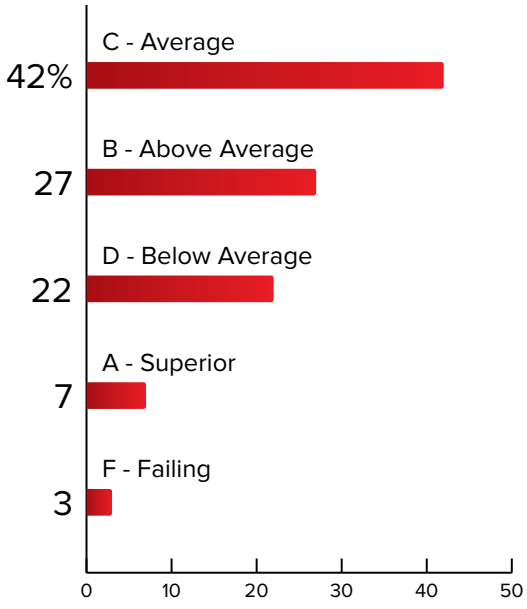
Which begs the question: Which tools have organizations deployed?

Which incident prevention/detection/investigation tools does your organization currently use?



The common solutions are the traditional ones – the ones that industry experts say are no longer effective against advanced adversaries: endpoint anti-malware, network anti-malware and email anti-malware. The common strength of these products is also their common weakness. They are effective against known threats. They are not designed to respond in real-time to new and emerging threats.

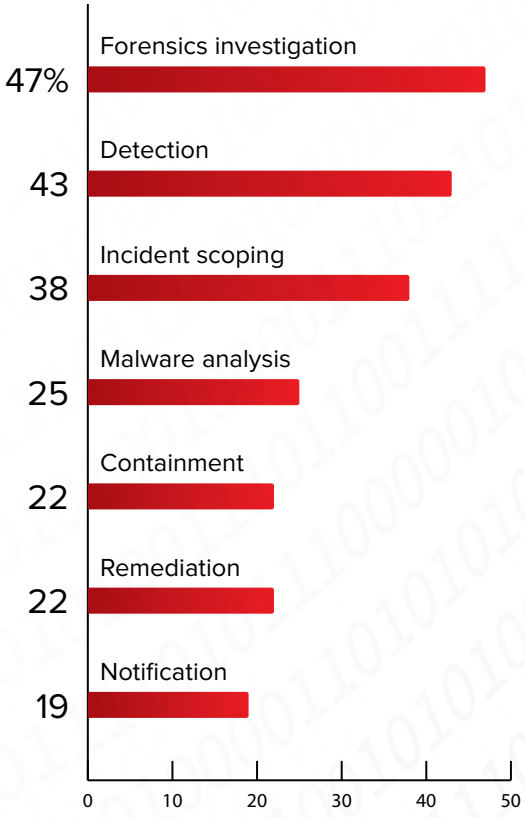
How would you rate the maturity of your organization’s breach response skills in relation to the skills of the threat-actors targeting your firm?



This may be one of the more telling statistics in the survey. When asked how their in-house breach response skills stack up against the skills of the threat-actors targeting their firms, 67 percent of respondents rate themselves average or below.

This point reinforces the common theme that survey respondents – despite general optimism about their capabilities – have an internal skills gap that must be addressed.

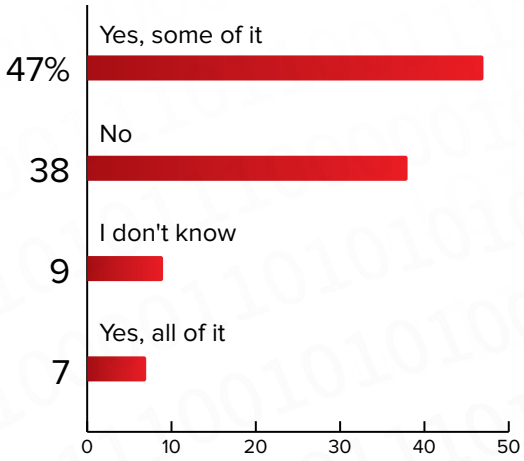
What do you believe are the biggest skills/process gaps in your organization's breach response program?



Asked to assess their internal skills deficit, respondents say that their biggest pain points are forensics investigation, breach detection and incident scoping.

So, how are organizations addressing this deficit, both externally and in-house?

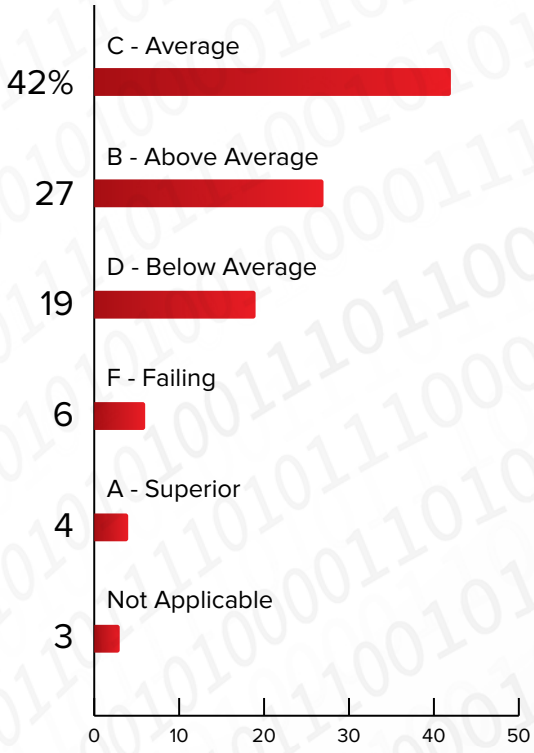
Do you outsource all or part of your detection and/or breach response activities?



Currently, 54 percent of organizations are outsourcing some, if not all, of their breach detection and response activities.

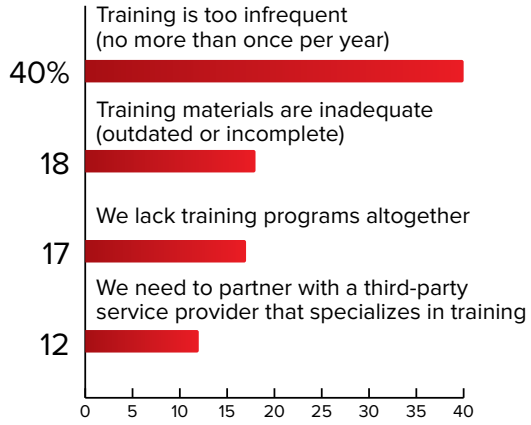
But they also are engaging in some in-house awareness and training activities ... to mixed results, as shown below.

How would you rate the effectiveness of your current security awareness/training programs for breach preparedness?



Security awareness/training is mandated by many regulatory agencies, and it always emerges in surveys such as this one as a key priority for the year ahead. Yet, when asked to rate the effectiveness of their current training programs, 67 percent of respondents say theirs are average or below. Only 4 percent say their programs are superior.

What is the biggest weakness of your current security awareness/ training programs for your incident response staff?



The biggest problem with training: Infrequency. Forty percent of respondents say their training is no more than once per year, and then 18 percent say the training materials are incomplete or outdated. Nearly one-fifth lack training programs altogether.

So, with these challenges in mind for context, how do organizations see 2016 taking shape? The next and final results section dives into the 2016 breach preparedness and response agenda.

FOCUS ON TOOLS & SKILLS

What's Missing?

Survey Analysis by FireEye CTO Grady Summers

Q: What do you find deficient about the security tools organizations are currently deploying?

Grady Summers

GRADY SUMMERS:
You know, organizations do still invest in technology that's maybe not helping them as much as they'd like. I think one problem we see is that a lot of tools are still signature-based. And those of us who work in the industry have seen over the last few years that signature-based tools are just completely overwhelmed. They can't keep up with how quickly attacks are evolving now. So I think that's one major deficiency.

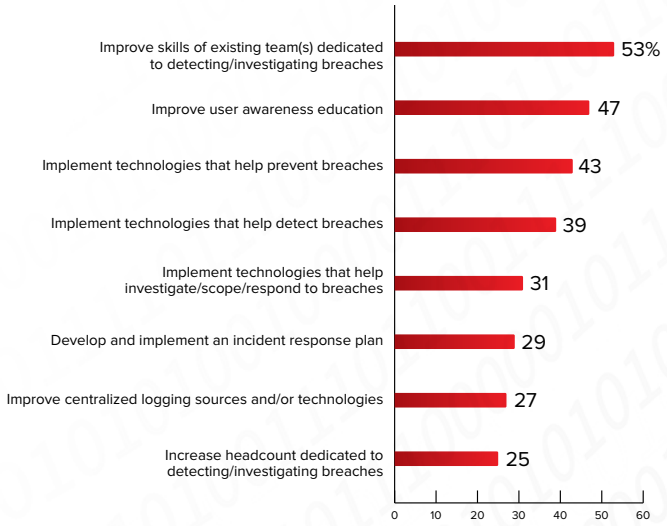
Another one I see, though, is that a lot of parts are not retrospective. And what I mean by that is they will give an alert at a certain point in time, but that doesn't leave an organization with a lot to work from. You can't then go back and rewind and replay the DVR, so to speak, to see what happened. And that's where we're trying to invest very much in our tools in the FireEye suite, for example, being able to go back and be retrospective. And we're certainly not the only vendor that does this, but our network forensics tools and our host forensics tools and our log forensics tools really focus not only on generating alerts, but giving you a context you need to actually solve the problem and to go back in time to look at the entire conversation that the user might have been having with, you know, a post on the Internet. And so I think that's an important aspect for orgs to consider when they purchase tools now.

V. 2016 Agenda

This report began with a note of optimism, and it ends with one. Given expected budgets and investment plans, there is good news in the year ahead. Namely:

- 98% will see same or increased budget in 2016
- Top 3 planned tech investments:
  - » Endpoint anti-malware
  - » Endpoint exploit detection/prevention
  - » Network forensics

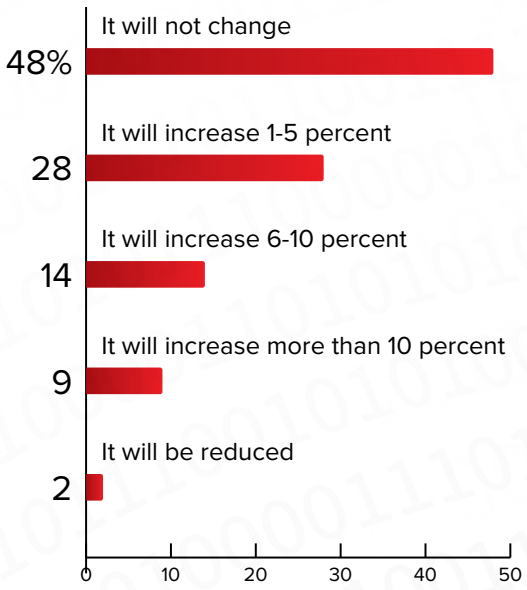
What do you believe must be your organization's top 3 breach response priorities for the coming year?



Asked to list their top three breach response priorities for the year ahead, respondents start with improving the skills of their existing teams dedicated to detecting/investigating breaches (53 percent).

The other two top priorities: Improve user awareness education (47 percent), and implement technologies that will help prevent breaches (43 percent).

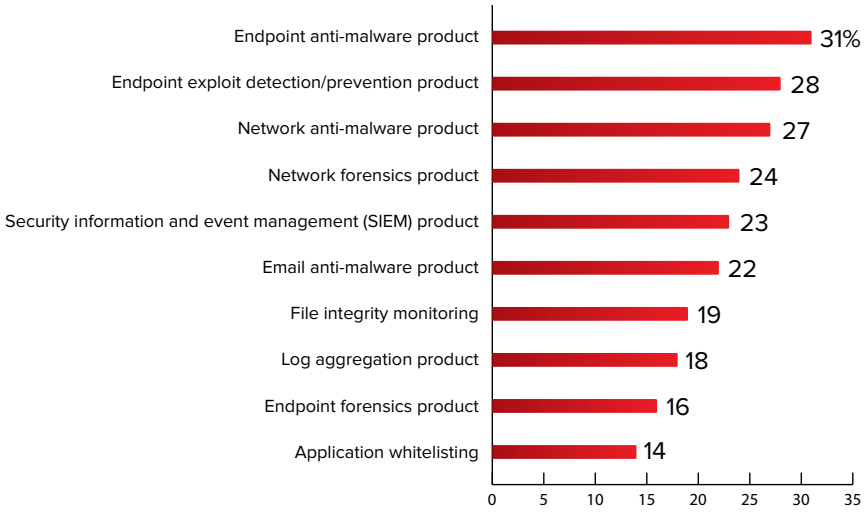
How will your breach response budget change in the coming year?



The smallest number here is the most important. Only 2 percent of organizations say their breach response budget will be reduced in 2016. The remaining 98 percent expect to receive at least as much as in 2015, or increases that range from 1 percent to more than 10 percent.

How will these funds be invested?

Which incident prevention/detection/investigation tools will your organization purchase?



On one hand, many respondents say they are investing in the tools they already have: endpoint anti-malware and network anti-malware products.

But they also plan to invest in endpoint exploit detection/prevention products, which should improve capabilities to spot attacks when they are launched. And network forensic product investments should improve the abilities to respond.

Next, the report will culminate in some final conclusions, and then Grady Summers, SVP and CTO of survey sponsor FireEye, will offer analysis and insight on how to put these survey results to work.

FOCUS ON 2016 AGENDA

Bang for the Buck

Survey Analysis by FireEye CTO Grady Summers

Q: In your view, what are the technology investments that really can make the biggest positive difference?

Grady Summers

GRADY SUMMERS: Technology at the email gateways can stop a lot of those [attacks] from coming in. So I think investing in the front vector of the attack life cycle is a place where organizations can get a lot of bang for their buck with email protection. Advanced malware protection - again, organizations should invest in having technology to see malware and stop it before it ever gets to the users' desktop. That's absolutely money well spent.

And then there's also the fact that many organizations are missing the capability for retrospective analysis, to be able to do log analysis, packet capture and post-forensics. I think those are the three areas of technology investment that can make a big difference.

Conclusions

Among the resonant points hammered home by the survey results:

1. Organizations Have Made Strides, But...

Adversaries have made greater strides. In the two years since the original ISMG/FireEye survey, it's clear that security leaders have learned more about their adversaries, and they now exhibit more self-awareness about their own preparedness and response capabilities. But awareness is one thing; action is another. It's time for organizations to close the security gap between themselves and their attackers.

2. Threat Intelligence is Key

And must be improved. It's disconcerting to see security leaders rate the value of their current TI so low. The sources of intelligence must be improved, as must the abilities to process and respond to the data efficiently and effectively. Security leaders must start by evaluating their current sources of threat intelligence, and then determine which new tools, skills or services will improve how that data is used to improve defenses.

3. Response Needs to Catch up to Detection

Too much damage can occur in too little time. While organizations have improved their ability to detect traditional attacks, they need more than the traditional security toolkit to more efficiently and effectively detect today's attacks. And then they need to be prepared to respond just as quickly and thoroughly with a combination of security tools, skills and services.

4. Staff/Skills Must be Enhanced

Organizations revealed a need to enhance their skills to detect attacks and then be able to investigate them with appropriate forensics capabilities. Some of this can be done in-house, but organizations also must be prepared to blend in-house and outsourced resources to match adversaries' expertise. The cliché is that people are the weak link in any security program. And these survey results show this to be true – organizations are hampered by the skills and expertise of their current staff. Awareness/training and even recruiting efforts can help, but a quicker fix might be to explore further investment in third-party services – which also brings access to new detection and forensics tools, as well as threat intelligence.

For more results and analysis from the 2015 Breach Preparedness and Response Study, please see: http://www.bankinfosecurity.com/webinars.php?webinarID=760

SURVEY ANALYSIS

How to Improve Breach Preparedness and Response

Survey Analysis by Grady Summers, SVP and CTO, FireEye

In preparation of this report, ISMG VP Tom Field sat down with FireEye SVP and CTO **Grady Summers** 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.

Summers is the Senior Vice President and Chief Technology Officer at FireEye. Prior to joining FireEye/Mandiant, Summers was a Principal in Ernst & Young's information security practice. Before E&Y, Summers was the global CISO at General Electric. Summers has consulted with dozens of Fortune 500 companies, specializing in governance, program management, and SOC/CIRT development.

How Attackers Have Improved Their Game

Q: From your perspective, how have the attackers improved their game in the past two years?

GRADY SUMMERS: We see attackers now adopting techniques that we used to only see in the really advanced state-funded types of attack groups. And what I mean by that is, going back several years, we might see a financial attack that was more of a smash-and-grab or very quick in-and-out type attack. But those financially motivated attackers have now adopted the long-term persistence and the sort of low-and-slow techniques that we used to just see in state-sponsored attackers. More specifically we're seeing a lot of creativity among attackers. They're adapting very quickly.

Just a few weeks ago, we released a report on a Russian group and a campaign we call HAMMERTOSS. And HAMMERTOSS is unique because rather than traditional command-and-control type infrastructure, they extensively use social media, and so their stage-one command-and-control is on Twitter. They would then point the compromised machines to pick up an image on GitHub to obtain further instructions, and they would exfiltrate or steal data and upload it out to a cloud storage software.

So you can see this evolution from kind of old school, traditional, rigid command-and-control servers to very flexible and difficult to detect techniques using social media. Which, of course, makes it a lot harder for all of us defenders out there.

How Have Defenders Improved?

Q: How have targeted organizations improved their defenses in that same two-year time period?

SUMMERS: I'm struck now by so many organizations that are starting to build security operations centers that we might have only seen in the financial services, the defense industry, five years ago. And now I'm seeing those types of SOCs being built in retail and healthcare and the energy sector. So that's encouraging.

"We see attackers now adopting techniques that we used to only see in the really advanced state-funded types of attack groups."


Grady Summers

There's more investment in types of tools. I think probably more importantly, though, there's investment in developing people. We hear a lot about the talent shortage out there, but we see organizations really upping their game by starting to make long-term investments, training folks and getting people earlier in their careers and attracting them into security and training them right.

Biggest Gap Between Hunters and Hunted?

Q: What do you see as the biggest security gaps between the attackers and the attacked?

SUMMERS: I sometimes joke that some of the gaps we talk about are the same ones I've been talking about for the last decade. There's newer technology to help solve some of them, but by and large attackers have been exploiting a lot of the same things. One of those is email. Spear-phishes are the number-one way that attackers are getting into organizations, and that seems to just continue unabated. Attackers are still getting in pretty easily with well-crafted spear-phishing emails.

But a lot of the big gaps we see are just kind of around the basics, or hygiene. For example, we still talk a lot about network segmentation, and many organizations that we respond to at FireEye, when they have an incident, we learn that their very sensitive PII about their customers, or their sensitive intellectual property, is on the same network as their external-facing web servers, for example. We still see very flat networks, which make it much easier for attackers.

Lack of two-factor authentication continues to be a big gap, and that's not a sexy one to talk about. It's pretty much the basics, but as recently as the last few months we're responding to major organizations that have these Citrix environments and VPN environments, and still have single-factor authentication, and that makes it really easy for attackers.

Survey Findings: Gut Response

Q: You've had a chance to look over the survey results and draw your own conclusions. What's your gut response?

SUMMERS: A few things jumped out to me. It was interesting that 48 percent of companies rate themselves at above average or superior in terms of incident response capabilities. It's disappointing that only half of organizations think they're above average. That tells me that a lot of orgs have a fairly low opinion of their capabilities. But what's probably more interesting about that is that we don't really know what "average" means in our industry. It's difficult to really put a score or measurement on how an organization does incident response. You know, we have an annual report, and last year we found that the median amount of time that an attacker was on the victim network was 205 days. So if we use that as a definition of average … then the benchmark is pretty low. And that's concerning.

Gap Between Detection and Response

Q: One of the things that really leapt out to me was the difference between the speed in which organizations can detect an incident and then the time that it takes them to respond.

SUMMERS: I noticed that as well. But it's actually not surprising to me. When we work with organizations on improving their incident response processes, we often find that there has been attention

"It's disappointing that only half of organizations think they're above average. That tells me that a lot of orgs have a fairly low opinion of their capabilities."

dedicated to finding things – and, really, that's where a lot of technology that organizations acquire comes in. They're looking for a new idea, alerts or new ways to detect attacks. So a lot of focus on that detection, which is very good.

But organizations again don't necessarily know what to do after the fact, and so we'll often map out a company's incident response process and we'll find that a lot of time is wasted on seemingly mundane things like collecting a triage package or a live response from a host. And many organizations don't have that process automated. So an analyst is taking an alert and then trying to figure out manually, "how do I get a set of tools up to the desktop damage?" We're also seeing, you know, again, very basic stuff. But a lot of organizations get hung up on things like asset identification. So that's not at all an exciting one to talk about. But we see it again and again. The incident response process is about having a documented process to begin with and really just doing the basics well, and too often organizations haven't invested in that part of the process.

"The incident response process is about having a documented process to begin with and really just doing the basics well, and too often orgs haven't invested in that part of the process. "

Awareness & Training

Q: How much of a positive difference can good training actually make?

SUMMERS: Well, I'll start by saying that security awareness training is a good thing that most organizations have to do because they're bound to it by compliance, and it certainly doesn't hurt. But the next thing I'll say might be a little more controversial. And that is, honestly, I think most of these programs are a complete waste of time. Here's the problem: If you were to give me an hour, I could develop a spear-phish with a never before seen malware that will coast right through any signature-based system. And I could probably compromise any leader at a Fortune 100 company. The attackers have the time. They've got the expertise. When they're targeting a particular organization, they're going to develop a spear-phish that will get through and it will be contextual. That will be something that an executive or a research leader or their assistant is going to click on.

So I don't want to be fatalistic about it, but the fact is: You can have 99 percent of your organizations understanding what threats are and not clicking on attachments and reporting things when they see it and all that. But it only takes one person to click.

So, like I said, it doesn't hurt to do training, and I think most orgs will continue to do it, but I think there's a lot of false hope placed in security awareness programs.

Put Survey Results to Work

Q: How should security leaders read and analyze these survey results that we've gone over today?

SUMMERS: I think there's a pretty clear call to action there from what we see as a majority of organizations know that they're being targeted; that attackers have motives that range from stealing their intellectual property to disrupting their operations. But then half of the respondents say that they know they're not doing enough, that their antimalware protection is insufficient; their incident response capabilities are below average; [and] their people and expertise isn't where it needs to be.

And so I read this as almost a perfect storm as the attacks are ramping up. Organizations are more targeted than ever. But they're also, by their own admission, not capable of defending. So this is great information that security leaders can use to help make senior management aware of the state of where they are, but also seems to be a really clear call to me that more needs to be done.

The message is that attacks are not always possible to stop, but they can be mitigated. The impact can be mitigated with the right investment in detection and response.

Organizations have got to gather the right information so that if and when the inevitable happens, they're ready to respond to it. But, you know, despite all the gaps that we've talked about, I think the good news is there's hope. I've worked with hundreds of orgs over my consulting career, and there are ones who start to make principal investments in this area in training their people, and the good news is: You can absolutely turn the corner and start to push the attackers back on their heels. They're responding more quickly, and so organizations who choose to invest in the space with money and effort can really make a difference.

For more results and analysis from the 2015 Breach Preparedness and Response Study, please see: http://www.bankinfosecurity.com/webinars.php?webinarID=760

Want to learn more about breach preparedness and response?

Check out these content resources.

One on One with FireEye's Dave DeWalt

"It's a tough conversation, telling [clients] they've spent a lot of money on defense-in-depth that isn't working," says FireEye CEO David DeWalt. "If they don't change, they're risking their company."

http://www.inforisktoday.com/interviews/one-on-one-fireeyes-dave-dewalt-i-2499

Advanced Threats: Improving Response

In the wake of the APT30 report's revelations, FireEye's Ranndeep Chonker talks about the Indian government's approach to information security and its primary challenges in dealing with APT types of attacks.

http://www.bankinfosecurity.asia/interviews/advanced-threats-improving-response-i-2835

Inside An Elite APT Attack Group

How does an advanced threat adversary operate for 10 years, undetected? FireEye APAC CTO Bryce Boland shares details of the decade-long APT30 campaign that targeted organizations in India and Southeast Asia.

http://www.inforisktoday.com/interviews/inside-elite-apt-attack-group-i-2726

Why 'Adaptive Defense' Is Critical

As hack attacks, such as the breach of Anthem Inc., become more common, it's more critical than ever for organizations to carry out an "adaptive defense model" to protect sensitive information, says Dave Merkel, former chief technology officer at FireEye.

http://www.inforisktoday.com/interviews/adaptive-defense-critical-i-2574

RESULTS WEBINAR

2015 Breach Preparedness and Response

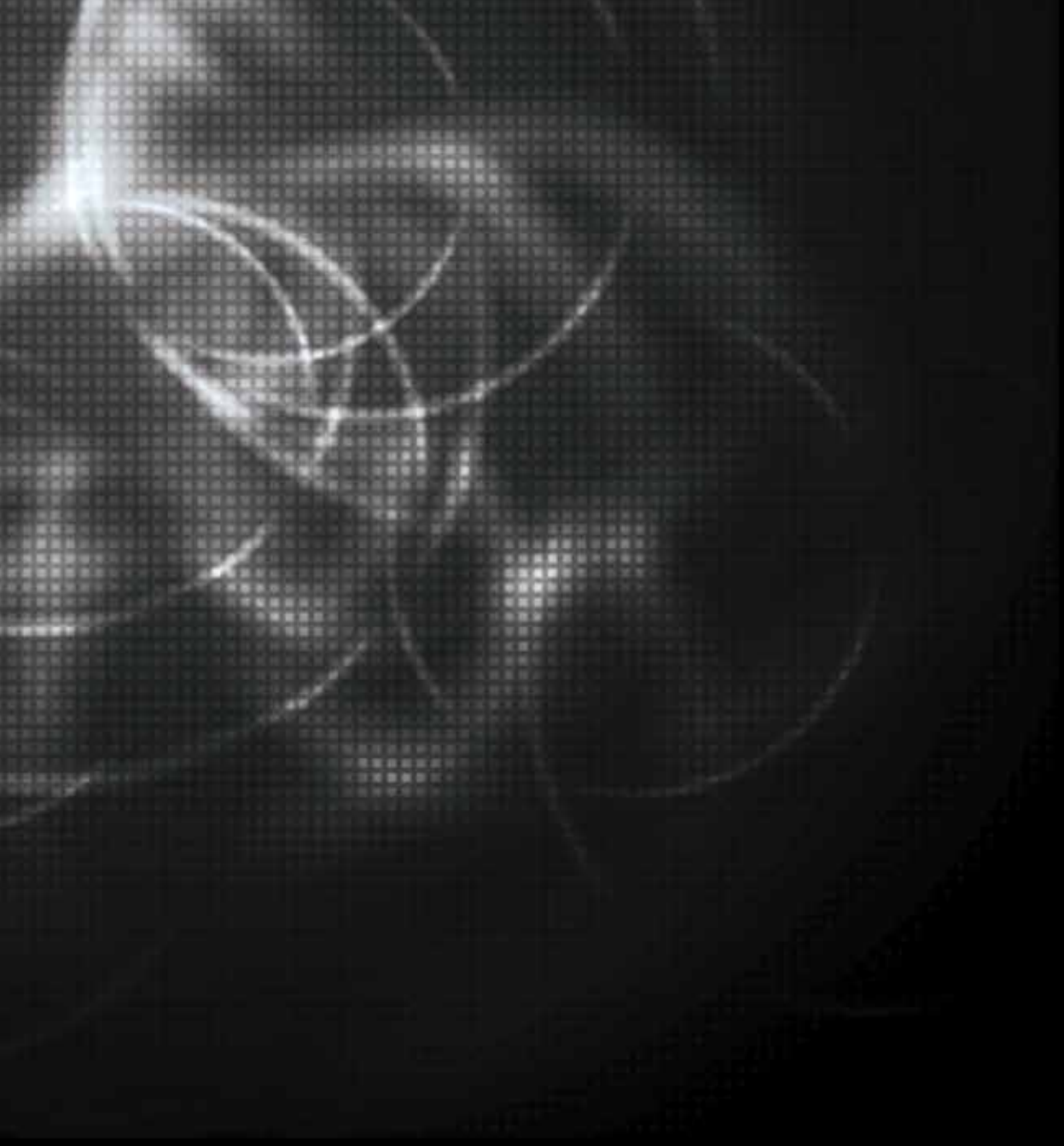
Presented by Grady Summers and Tom Field

How well prepared are organizations to respond to a potentially devastating data breach - such as the likes that hit Anthem, OPM or even Ashley Madison? Are their security programs and controls truly as effective as security leaders believe them to be? These are among the questions answered by the results of the 2015 Breach Impact Study.

Join FireEye CTO Grady Summers, and ISMG VP Tom Field, for an overview and analysis of this important new survey, with emphasis on:

- Where organizations are most and least prepared for an attack;
- Current security controls deployed for detection and response;
- The 2016 agenda: What are the top planned investments for improved breach response?

REGISTER NOW: http://www.bankinfosecurity.com/webinars.php?webinarID=760



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

902 Carnegie Center • Princeton, NJ • 08540 • www.ismgcorp.com