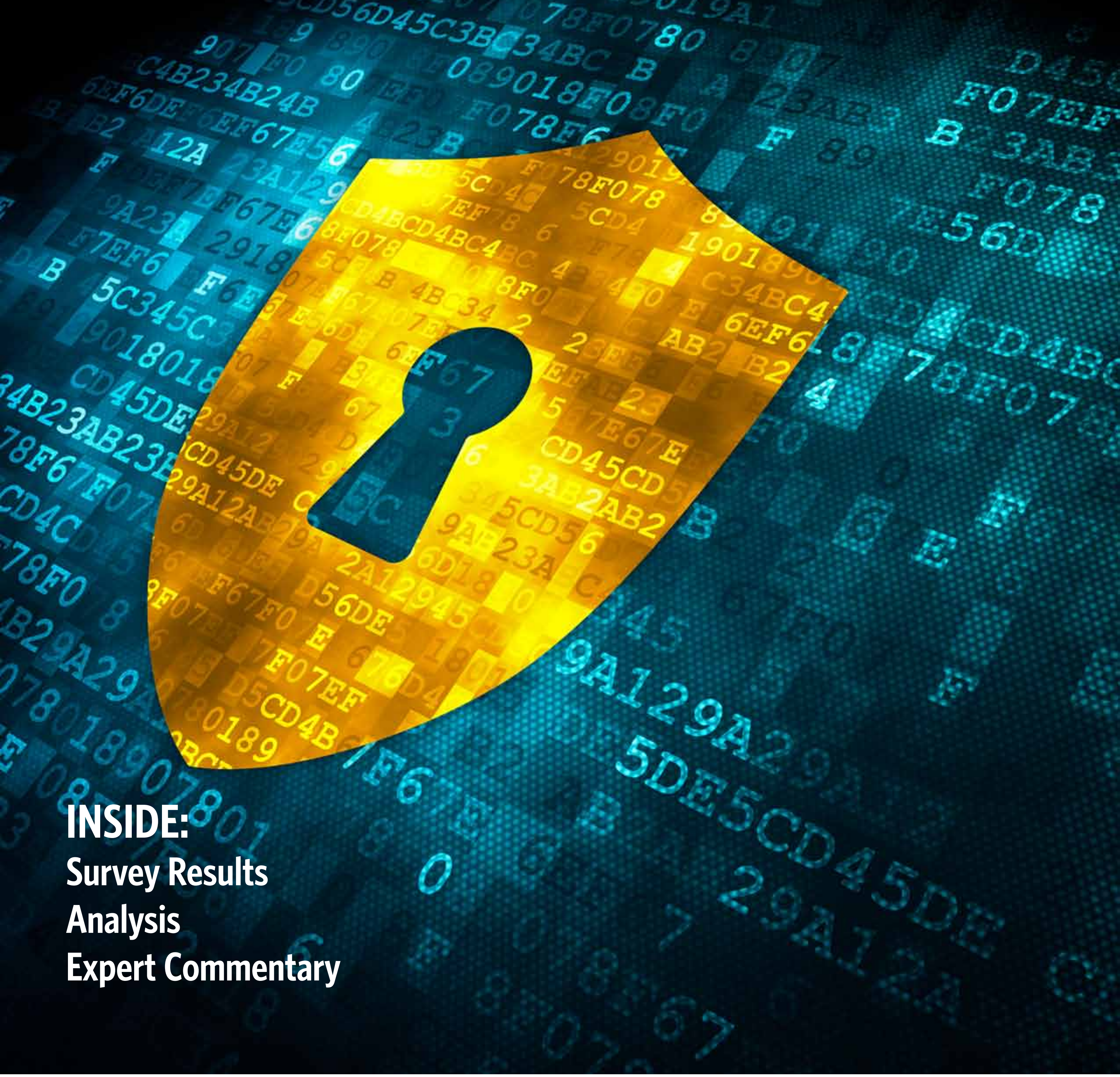
2013 Cyber Security Study

What is the Impact of Today's Advanced Cyber Attacks?



INSIDE:

Survey Results

Analysis

Expert Commentary

Bit9

iSMG
INFORMATION SECURITY
MEDIA GROUP

From the Editor

Stark Figures About Today's Advanced Threats

Tom Field
VP, Editorial

Here, in short, is why you need to be concerned about today's advanced threats:

- 47 percent of surveyed organizations know they have suffered a cyber attack in the past year;
- 70 percent say they are most vulnerable through their endpoint devices;
- And yet 52 percent rate at "average-to-non-existent" their ability to detect suspicious activity on these devices.

With those points in mind, welcome to the 2013 Cyber Security Survey, commissioned by Bit9 and conducted by Information Security Media Group.

From the board room to the data center, global organizations are increasingly aware of the damage that can be caused by today's most sophisticated cyber attacks, including the advanced persistent threat, targeted attacks and malware.

But how equipped are these organizations to detect and defend against cyber attacks before they take root in endpoints and servers? That is the question we answer in the pages ahead.

In addition to the survey results, please pay heed to the expert analysis from Bit9 CSO Nick Levay.
Please don't hesitate to share your reactions to these survey results and analysis.

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

Table of Contents

2013 Cyber Security Study

What is the Impact of Today's Advanced Cyber Attacks?

Introduction

Survey Results

Sponsored by

Bit9

Bit9 is the leader in a new generation of endpoint and server security based on real-time visibility and protection. Bit9 is the only solution that continuously monitors and records all activity on endpoints and servers and stops cyber threats that evade traditional security defenses. Bit9's real-time sensor and recorder, cloud-based services, and real-time enforcement engine give organizations immediate visibility to everything running on their endpoints and servers; real-time signature-less detection of and protection against advanced threats; and a recorded history of all endpoint and server activity to rapidly respond to alerts and incidents. http://www.bit9.com

Top 3 Challenges for Today's Security Teams

Why First-Generation Solutions Are No Longer Sufficient

By Nick Levay, CSO, Bit9

The results from the 2013 Cyber Security Survey echo the challenges that we hear from customers each and every day.

A resounding 47 percent of organizations surveyed report that they suffered at least one cyber attack in the past year. But what is even more astounding is the 13 percent of respondents who say they do not even know if they have been attacked.

This uncertainty is well-founded—according to the 2013 Verizon Data Breach Investigations report, 66 percent of breaches in 2012 took months or even years to discover. When found, 69 percent of breaches were spotted by an external third party (like the FBI, Secret Service or forensic services) rather than by in-house staff. Why does this security landscape exist? The 2013 Cyber Security Survey identifies three challenges facing security teams today:

» 1. First-generation security solutions cannot protect against today's sophisticated attackers;

» 2. There is no silver bullet in security;

» 3. There is an endpoint and server "blind spot."

First-Generation Security Solutions Cannot Protect Against Today's Sophisticated Attackers.

It seems like each day there is a new attack reported in the news: advanced attacks such as Flame, Gauss and the Flashback Trojan that attacked 600,000 Macs. These "public" cyber attacks are, unfortunately, just the tip of the iceberg. The number and variety of attackers and their differing goals and motivations are overwhelming.

The 2013 Cyber Security Survey shows proof that traditional, signature-based security defenses cannot keep up with today's advanced threats and malware:

- 66 percent of survey respondents say their organizations' ability to protect endpoints and servers from emerging threats for which no signature is known is "average" to "non-existent."

- 40 percent of respondents state that malware that landed on their endpoints and servers got there because it bypassed antivirus.

First-generation security solutions, such as signature-based antivirus, can't keep up with the tidal wave of widely targeted malware (400+ million variants), let alone advanced attacks that target specific organizations.

© 2013 Information Security Media Group

Nick Levay

There is No Silver Bullet in Security.

In speaking with customers, we've learned that organizations increasingly rely on new-generation network security solutions as a primary defense against cyberthreats. This is a step in the right direction, but not a silver bullet. According to the survey:

- 27 percent of respondents say malware was able to land on their endpoints and servers because it bypassed network security.
- 30 percent responded that they don't know how it got there.

The digital assets that you need to protect reside on your endpoints and servers, or are at least accessible from your endpoints and servers, and it is inevitable that some malware is going to make it to this critical infrastructure. How does it happen? It could be that a user fell victim to social engineering, a laptop was disconnected from your network and network security, a user plugged in an infected USB device or mobile phone to his or her PC, or an advanced threat slipped past your AV.

To combat the APT, you need to fortify your endpoints and servers with security solutions that work together to give you a unified, holistic approach. A defense-in-depth strategy is necessary, where you are not counting on just one security control to stop an attack.

There is an Endpoint and Server Blind Spot

The survey results indicate that there is also an "endpoint and server blind spot."

- 59 percent say that when it comes to real-time monitoring of files that attempt to execute on servers and endpoints, their organizations' abilities rate from "average" to "non-existent."
- 61 percent say that once a file is determined to be malicious, the organization's ability to determine how many endpoints and servers are infected rates from "average" to "non-existent."

© 2013 Information Security Media Group

» Only 37 percent rate their organizations' ability to create a history of activity for use in forensic investigations as "very good" or "excellent."

These statistics are in line with what we hear from our customers: Security teams have limited to no visibility into what is happening on their endpoints and servers. If malware is suspected, there is no way of knowing which machine it's running on, if it executed or what it is doing. There are often no historical details to determine when a threat arrived and executed, leading to slow remediation.

A New Generation of Security

It is clear from the 2013 Cyber Security Survey that it's no longer a matter of if an attack will happen to your enterprise, but really a matter of when. So what can you do to prevent an attack from happening in your organization? And how can you ensure you collect the information necessary to detect when a compromise occurs?

Organizations need a new generation of endpoint and server security that is based on real-time visibility, actionable intelligence and protection. By adopting such solutions, organizations gain immediate visibility to everything running on their endpoints and servers; real-time signature-less detection of and protection against advanced threats; and a recorded history of all endpoint and server activity to rapidly respond to alerts and incidents.

> Organizations need a new generation of endpoint and server security that is based on real-time visibility, actionable intelligence and protection.

Nick Levay is the CSO of Bit9, a leading provider of endpoint security solutions. Specializing in technical operations and cyber counterintelligence, he focuses on understanding actors, their tactics and risk exposure to organizations. He has more than 15 years of experience working in environments ranging from Internet service providers to think-tank organizations.

© 2013 Information Security Media Group

Hard Numbers

The survey captured a number of startling statistics, including the following:

47% Of surveyed organizations experienced a cyber attack in the past year.

13% Do not know if they were attacked in the last 12 months.

70% Believe they are most vulnerable through endpoint user devices, such as PCs, laptops and desktops.

© 2013 Information Security Media Group

What is the Survey About?

On a daily basis, organizations around the globe succumb to sophisticated cyber attacks. The impact of such attacks can range from a minor inconvenience to tremendous financial losses, as well as damage to an organization's reputation and its ability to function as a growing concern.

So, faced with the ever-growing sophistication of threat actors, how well-prepared are organizations to detect and defend against cyber attacks before they take root in the company's PCs, laptops, desktops and servers?

That question is the foundation of this study, which provides the following information:

» **What's the impact of today's advanced cyber attacks?** How often do cyber attacks take place, and what impact do they have on the victim organizations?

» **Where are organizations least prepared to detect and prevent advanced cyber attacks?** What types of "blind spots" exist, and how effective are organizations at preventing attacks of varying sophistication?

» **How effective are organizations at monitoring and responding to threats?** What tactics and tools do organizations deploy to monitor and respond to threats? How long does it take them to analyze an alert?

» **What are the cyber attack defense spending priorities for 2014?** How much do organizations plan to spend on their cyberdefenses, and where do they plan to invest the funds?

This survey was conducted online during the summer of 2013. Nearly 250 respondents participated in this international study. Key characteristics of the respondent base:

» 62 percent are from the U.S., with 10 percent from the UK and Europe;

» Top responding industries are:

- Banking/financial services – 36 percent
- Technology – 12 percent
- Healthcare – 10 percent

» 47 percent of respondent organizations employ 500 or fewer employees, while 22 percent employ more than 10,000.

» 59 percent of respondents deploy only Windows-based endpoints in their organizations, while 1 percent are all-Mac shops. The remainder offer a mix of endpoint devices, with 31 percent saying more PCs than Macs.

© 2013 Information Security Media Group

Impact of Today's Cyber Attacks

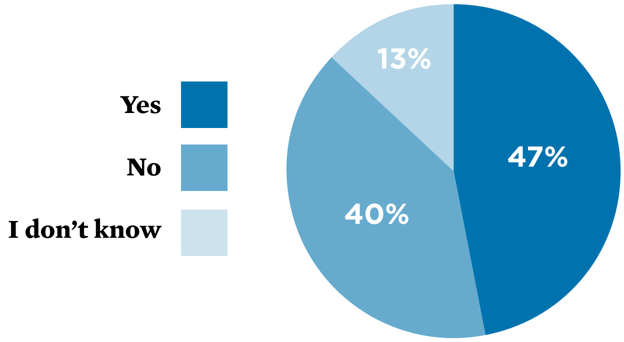
In this section, we will review survey participants' responses regarding the number that have experienced an attack in the past year, the impact of those attacks, and if applicable, how malware entered the organization's environment.

Survey participants report the following information:

- 47 percent have experienced a cyber attack in the past year.
- Of those organizations that reported a cyber attack, 33 percent experienced employee downtime/business disruption.

Key Findings:

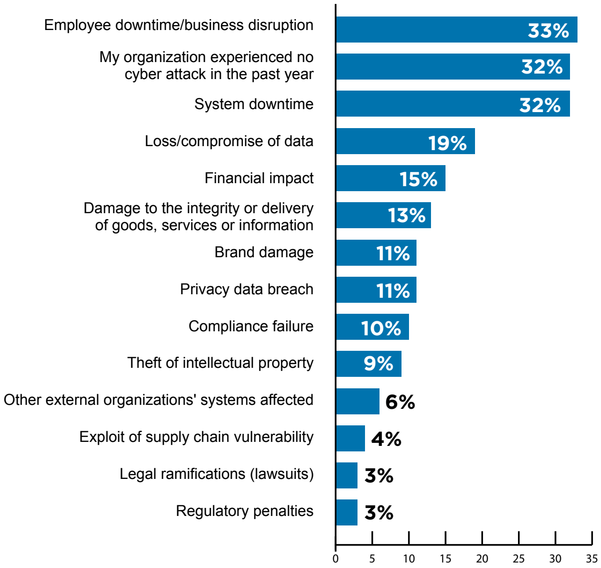
In the past year, has your organization experienced a cyber attack?



Almost half of the survey participants (47 percent) experienced a cyber attack in the past year. But 13 percent of organizations do not know if they experienced an attack at all – a troubling statistic that does not speak well of their abilities to monitor systems and detect threats.

As we will see in a subsequent section, respondents recognize that detecting evidence of a cyber attack presents challenges, especially on endpoint devices.

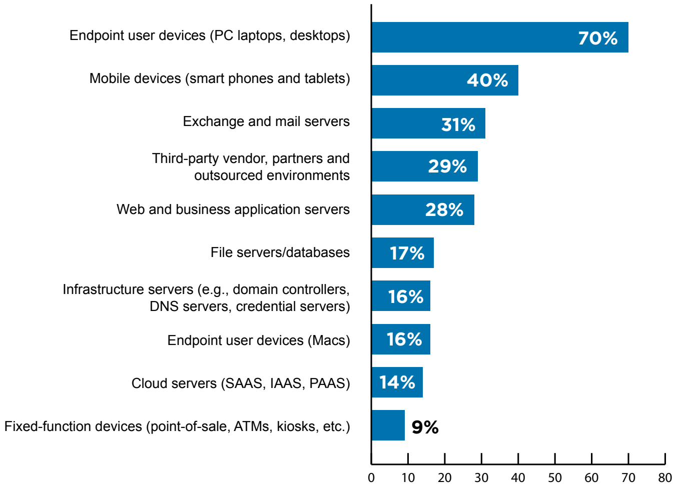
If your organization did experience a cyber attack, what was the impact of the incident(s)?



When subject to a cyber attack, the impact varied considerably; however, 33 percent report employee downtime/business disruption.

System downtime was a result for 32 percent, and 19 percent say they experienced a loss/compromise of data, while 15 percent report a financial impact associated with the attack.

Where in your organization do you believe you are most vulnerable to a cyber attack?



> 70 percent of organizations view endpoint user devices as their top vulnerability.

Some 70 percent of organizations view endpoint user devices as their top vulnerability. Mobile devices are next in terms of vulnerability, mentioned by 40 percent.

Exchange and mail servers place third at 31 percent.

With this benchmark information as context, let's now delve into the subsequent topics of detection and monitoring.

© 2013 Information Security Media Group

Detection

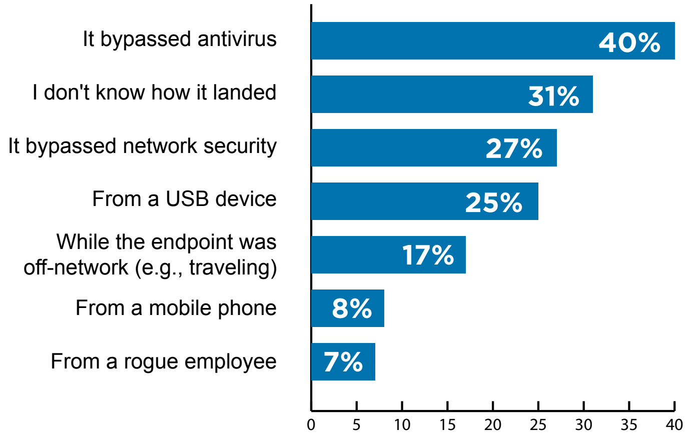
Detecting a threat before it has a chance to take hold within the organization's IT environment is where most companies should focus their efforts.

In this section of the study, we learn how effective organizations are at detecting threats, as well as gathering insight regarding their ability to detect the most advanced threats. Among the takeaways:

- Top 3 responses regarding how malware landed on endpoints or servers: Bypassed antivirus (40 percent), don't know how it landed (31 percent), bypassed network security (27 percent).
- Only 45 percent of organizations believe that they would immediately detect an advanced attack with no signature in real-time, or near real-time.

Key Findings:

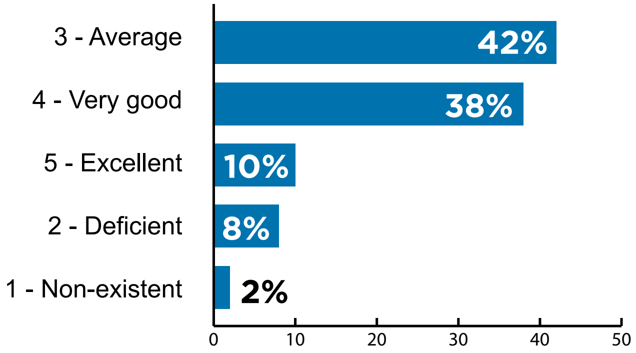
If malware has landed on your endpoints or servers in the past year, how did it get there?



When an attack involves malware, 31 percent of organizations don't know how it lands within their environment. For 40 percent of organizations, malware likely bypassed the organization's antivirus, while 27 percent report that it bypassed network security.

In 17 percent of attacks involving malware, the endpoint is off-network, which underlines the importance of protecting an organization's endpoints, regardless of their physical location.

On a Scale of 1 to 5, please rate your organization's ability to detect suspicious activity on endpoint devices before damage occurs.

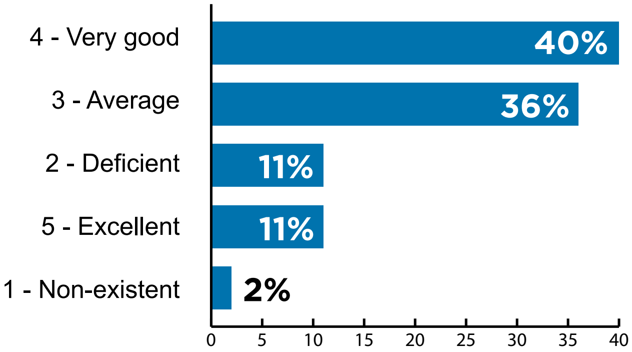


In total, 48 percent of organizations rate their ability as "very good" or "excellent."

But then look at the remaining responses: 2 percent of organizations respond that their organization's ability to detect suspicious activity on endpoint devices is "non-existent." Eight percent note that their ability to detect such activity is "deficient," and 42 percent assess their ability as "average." Combined, that means 52 percent of organizations assess their abilities as average-to-non-existent – a troubling statement.

© 2013 Information Security Media Group

On a Scale of 1 to 5, please rate your organization's ability to detect suspicious activity on servers before damage occurs.

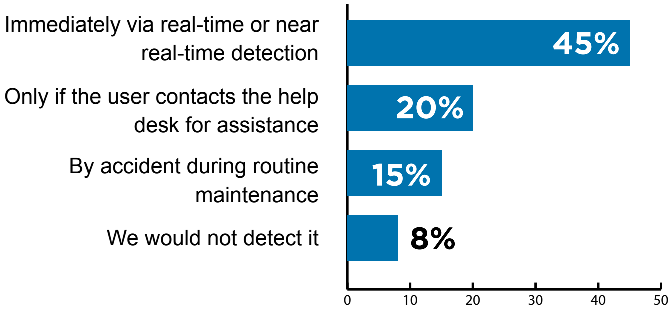


Survey respondents rate their ability to detect suspicious activity on servers as similar to their ability to detect activity on their endpoints.

In fact, 40 percent rate their ability as "very good," while 11 percent rate their ability as "excellent," both just slightly higher than the rates provided for endpoint detection.

However, 49 percent still assess their abilities as only average-to-non-existent.

If an advanced attack attempts to install malicious software on an endpoint or server for which there was no AV signature, when would your organization's security staff discover it?



Survey participants highlight their inability to detect advanced attacks with no AV signature.

Forty-five percent of organizations state that they would discover the threat immediately via real-time, or near real-time, detection. Eight percent note that they would not detect the attack, while 20 percent say they would only uncover the threat if a user contacted the help desk for assistance. Discovery via accident during routine maintenance accounts for 15 percent.

Clearly, many organizations are unable to detect advanced threats. So this represents an area of weakness, and potential improvement.

Next, we will review the findings about threat monitoring.

© 2013 Information Security Media Group

Monitoring

With an understanding of the number of cyber attacks organizations experience, and a sense of how they are positioned to detect such activity, we can now examine the study participants' ability to monitor and respond to threats.

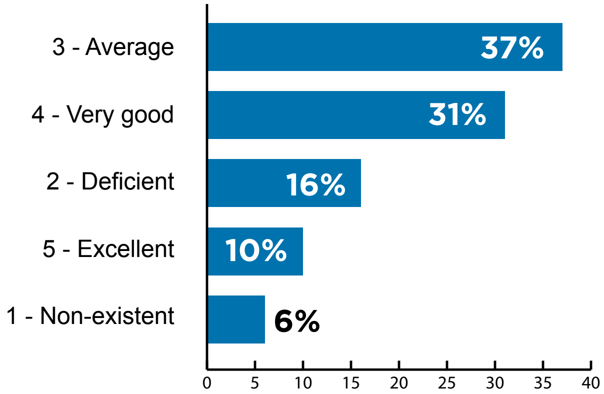
Responses to note in this section:

- 16 percent rate their ability to monitor files that attempt to execute on their servers and endpoints as "deficient."
- 60 percent of organizations manage between 0-99 alerts per day.
- 13 percent of organizations do not have a standard response time with respect to the analysis and response associated with an alert.

> Six percent of organizations rate their ability to monitor files attempting to execute on servers and endpoints as "non-existent."

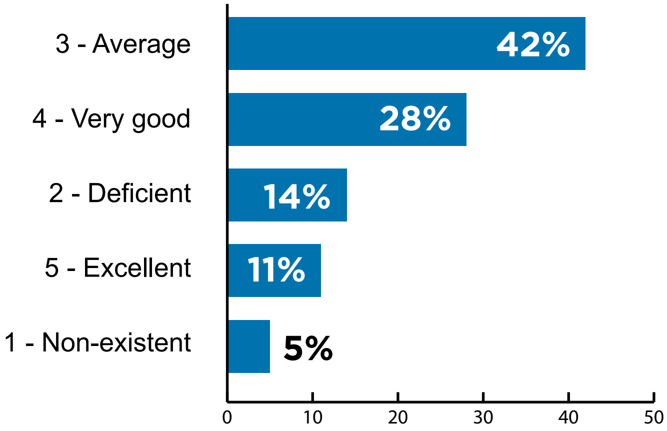
Key Findings:

On a scale of 1 to 5, how do you rate your organization's ability to monitor files - in real time - that attempt to execute on any of your servers and endpoints?



Most organizations rate their ability to monitor files attempting to execute on servers and endpoints as at least "average." However, 16 percent rate their ability to do so as "deficient," and 6 percent as "non-existent." Again, that's a combined 59 percent that rate their abilities as only average-to-non-existent. Hardly an endorsement.

In the event that your organization determines a file to be malicious, how do you rate your ability to determine - in real time - how many endpoints and servers it has infected?

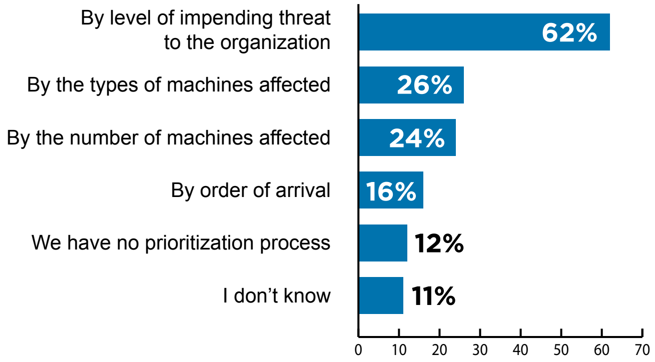


© 2013 Information Security Media Group

Fourteen percent note that their ability to monitor malicious file execution in real time is "deficient," while 5 percent respond that it is "non-existent."

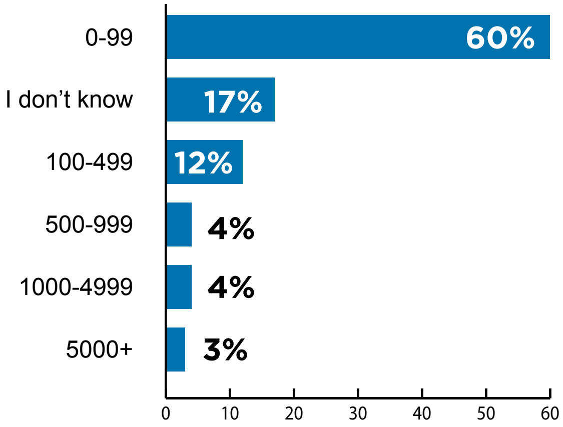
Given that 42 percent rated their ability as "average," in aggregate, 61 percent of organizations rate their abilities average-to-non-existent.

When one of your security technologies issues an alert, how does your organization prioritize its response?



Here respondents were allowed multiple answers to match their case-by-case prioritization. The vast majority (62 percent) note that they prioritize alerts based on the level of impending threat to the organization. Twenty-six percent prioritize by the types of machines affected and 24 percent by the number of machines.

On average, how many alerts do you get per day?



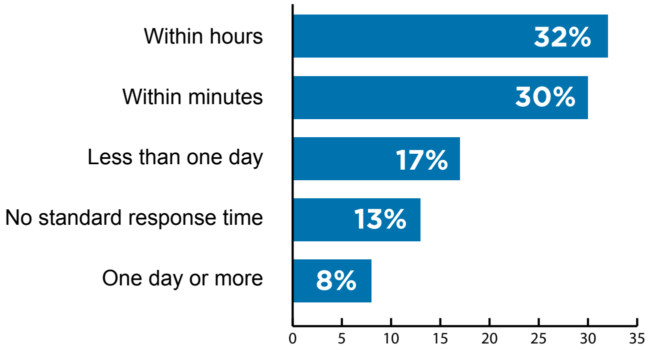
Most survey participants (60 percent) receive between 0 and 99 alerts per day. Only 3 percent receive 5,000+ alerts per day.

Seventeen percent of respondents do not know how many alerts their organizations receive.

© 2013 Information Security Media Group

Seventeen percent of respondents do not know how many security alerts their organizations receive each day.

How long does it typically take your organization to analyze and respond to a security alert?

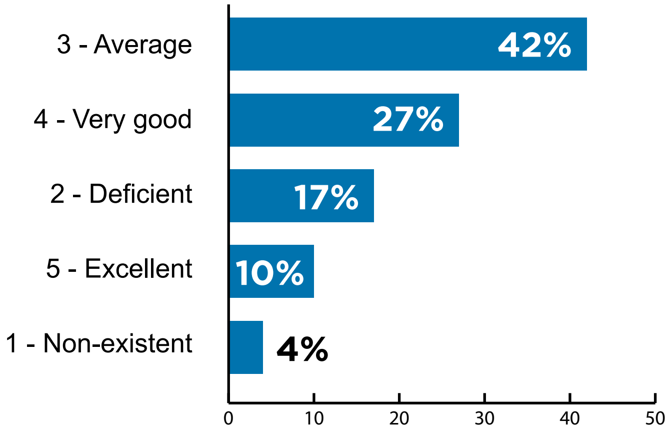


Responding to alerts is a measure of a company's ability to limit the damage associated with cyber attacks.

The majority of organizations surveyed respond within hours (32 percent), or minutes (30 percent).

Seventeen percent take less than one day, 8 percent take a day or more, while 13 percent of organizations do not have a standard response time in place.

On a scale of 1 to 5, how do you rate your organization's ability to create a history of activity on servers and endpoints (e.g., what files arrived in a given period, what executables ran, etc.) for use in a forensic investigation?



Only 37 percent of organizations rate their ability to create a forensic history on server and endpoint activity as very good or excellent. A combined 63 percent rate themselves at average-to-non-existent.

© 2013 Information Security Media Group

Protection

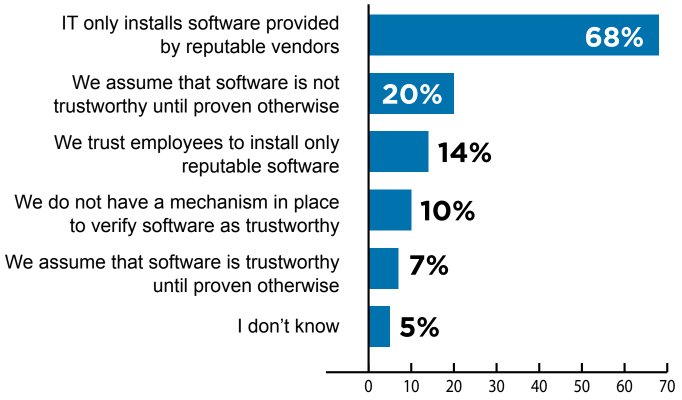
Detecting, monitoring and responding to threats are important elements in a company's defenses against cyber attacks. However, adopting protective measures can dramatically reduce an organization's exposure to cyber attacks and generate a considerable return on investment.

In this section, we'll learn what organizations do to prevent cyber attacks relating to their endpoints and servers, including the following:

- 43 percent of organizations have the ability to whitelist software on both endpoints and servers.
- 16 percent, however, don't know if they can whitelist software on their endpoints and servers.
- 59 percent have the ability to block writing, reading and execution of removable storage devices.

Key Findings:

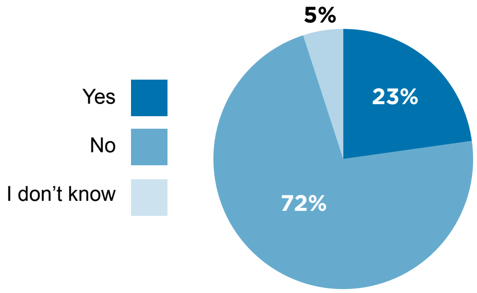
Assuming your organization has a process for authorizing software and applications to be installed, how does the organization determine what to allow?



Surprisingly, despite known threats from software installed by employees, 14 percent of organizations still trust employees to install reputable software, and 7 percent assume that the software is trustworthy until proven otherwise.

However, 68 percent only permit IT to install software from reputable vendors.

Does your organization currently allow the installation of software by end users without a review and approval by your security staff?

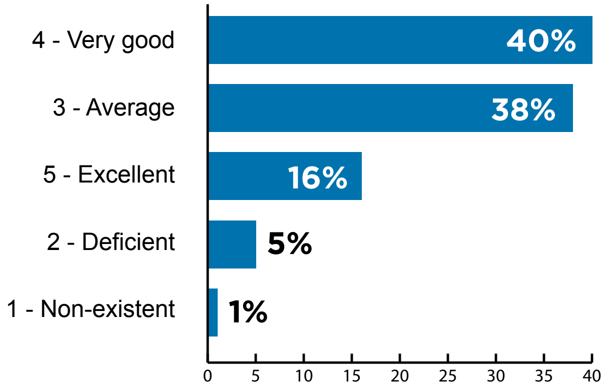


© 2013 Information Security Media Group

Nearly three-quarters of participants do not allow end-users to install software without a review and approval by their security staff. Only 5 percent are unaware of whether review and approval is necessary prior to a software installation.

However, 23 percent of organizations allow end-users to install software without review and approval by security staff. Consequently, nearly one-quarter of survey participants may be placing their organization at increased risk due to the lax controls associated with software installation.

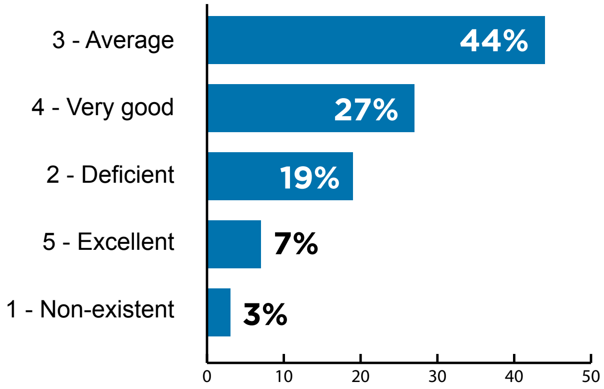
On a scale of 1 to 5, how do you rate your organization's ability to protect its endpoints and servers from known, signature-based threats?



Signature-based threats appear to cause minimal concern for organizations with 38 percent rating their abilities as "average," 40 percent as "very good" and 16 percent as "excellent."

Only 6 percent rate their abilities as "deficient" or "non-existent."

On a scale of 1 to 5, how do you rate your organization's ability to protect its endpoints and servers from emerging threats for which no signature is known (i.e., zero-day attacks)?



Organizations paint a much different picture when they consider attacks with no signature – which is how many of today's advanced threats present themselves.

Only 27 percent rate their abilities to protect against such attacks as "very good," compared to 40 percent for signature-based attacks.

The percentage that rates their abilities as "average" increases from

© 2013 Information Security Media Group

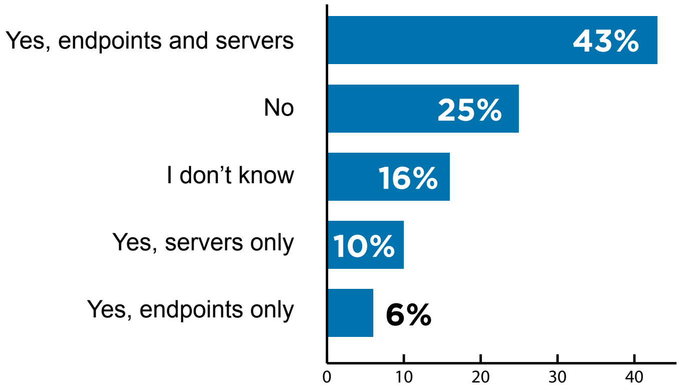
25 percent of organizations do not have the ability to whitelist software on either endpoints or servers.

38 percent for signature-based attacks to 44 percent for attacks with no signature.

And 19 percent rate their abilities as “deficient” when it does not involve a signature.

In all, 66 percent of respondents rate their abilities average-to-non-existent.

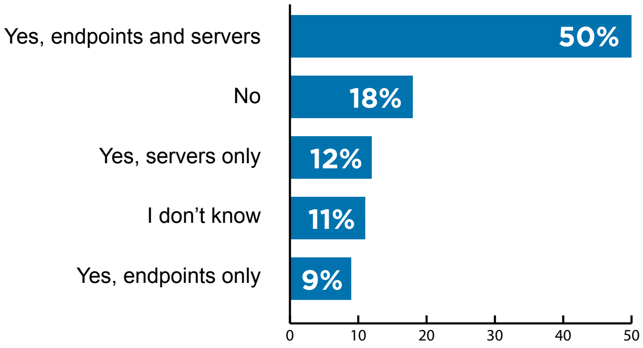
Does your organization currently have the ability to whitelist software you trust to run automatically on your endpoints and servers?



Most organizations possess the ability to whitelist software running on endpoints, servers or both.

However, 16 percent are not aware if they have the capability, and 25 percent do not have the ability to whitelist software on either endpoints or servers.

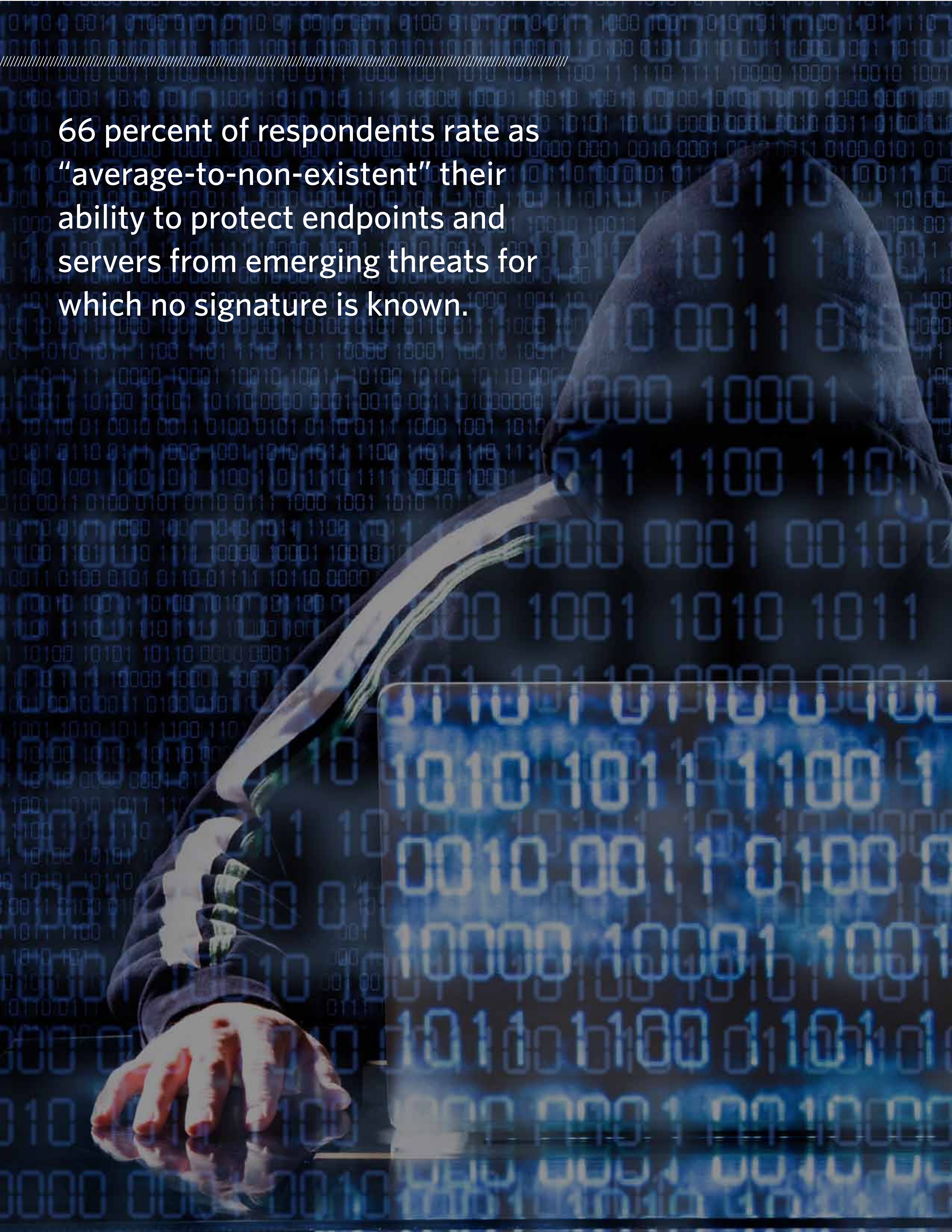
Does your organization currently have the ability to block unauthorized software from running within your environment?



Most organizations have the ability to block unauthorized software from running on both endpoints and servers.

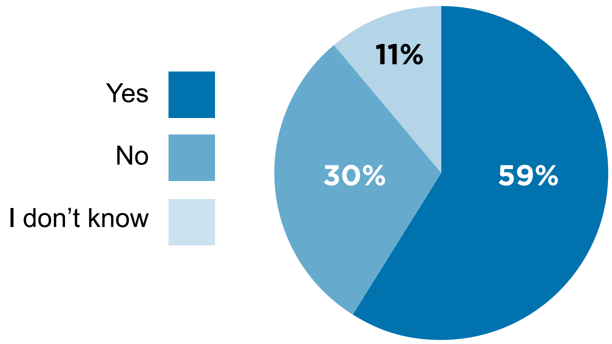
Eleven percent do not know if they can do so, and 18 percent state that their organization is unable to block unauthorized software.

© 2013 Information Security Media Group



66 percent of respondents rate as “average-to-non-existent” their ability to protect endpoints and servers from emerging threats for which no signature is known.

Does your organization currently have the ability to block writing, reading, and execution of removable storage devices on new and existing desktops and laptops?

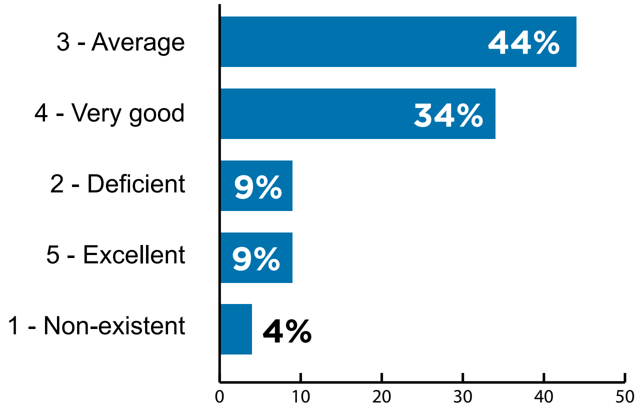


More than half of the organizations in our survey have the ability to block the use of removable storage devices. However, 30 percent do not have that ability, and another 11 percent do not even know if it's possible.

Removable storage devices not only facilitate the introduction of malware, they can also help an employee or third party steal data as well as intellectual property.

> 30 percent of organizations do not have the ability to block the use of removable storage devices.

On a scale of 1 to 5, how do you rate your IT security staff's ability to develop and customize endpoint security policies based on the needs of the business?



Many organizations give their IT security staff a passing grade, or high marks, when assessing their ability to develop and customize endpoint security policies.

Thirty-four percent rate their staff as "very good," and 9 percent rate their staff as "excellent" in this regard.

But, then, 57 percent of respondents rate their IT security staff's ability at just average-to-non-existent, which certainly is a concern when discussing the impact of advanced cyber attacks.

Against today's threats, average simply is not good enough.

© 2013 Information Security Media Group

2014 Cyber Security Agenda

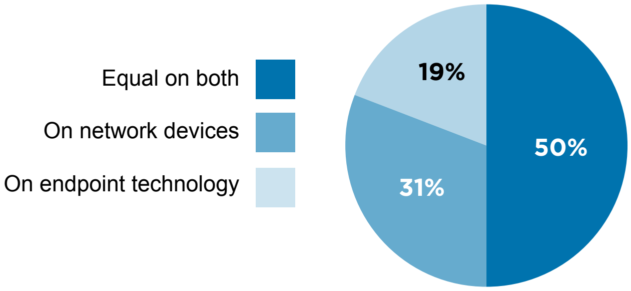
Where organizations plan to invest their cyber security-related dollars provides visibility to what is "top of mind" for participants in the coming year.

The following section provides predictions regarding the size of budgets, and the types of investments under consideration. Among the key considerations:

- 27 percent predict an increase in their cyber security budget of more than 5 percent.
- 44 percent say they will invest in awareness and training related to cyber security.

Key Findings:

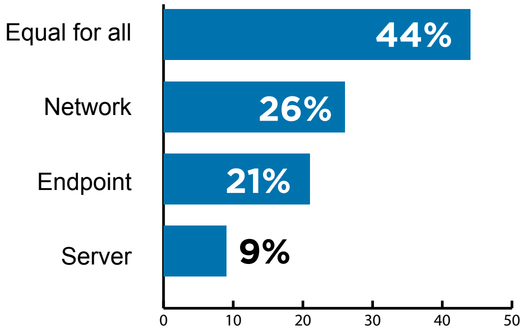
Over the past year, where have you made the majority of your security investments?



In the past year, 50 percent of organizations invested in both endpoint technology and network devices.

Thirty-one percent of organizations invested in network devices exclusively, while 19 percent allocated their investment funds to endpoint technologies.

What type of security technology do you feel has made the most advancement in the past five years?



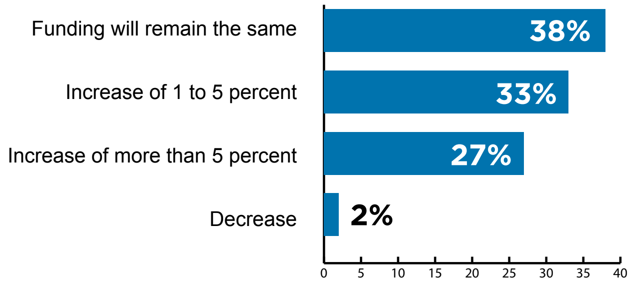
Forty-four percent of survey participants believe that endpoint, network and server security have kept pace with each other and that all three have improved at equal rates over the last five years.

However, 26 percent of participants believe that network security made the most advancement, and 21 percent select endpoint security.

Only 9 percent felt that server security made the greatest advancements.

© 2013 Information Security Media Group

For 2014, how do you expect your organization's budget to change when it comes to defending against cyber attacks?



Looking ahead ...

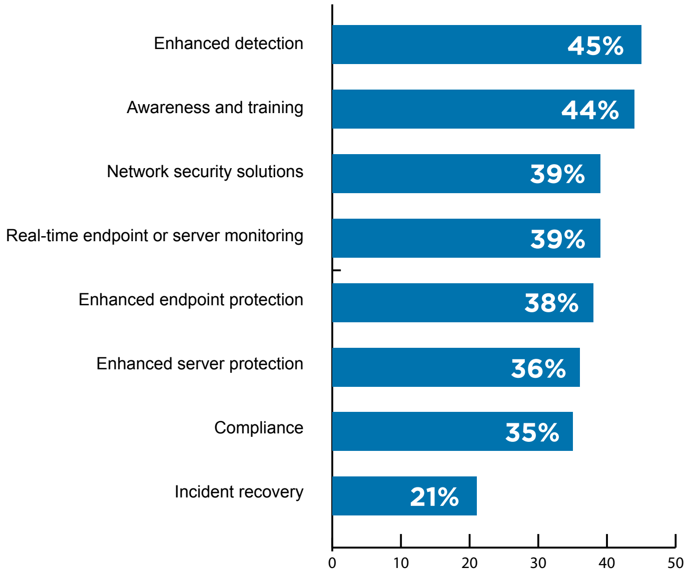
A third of organizations expect their budget for cyber attack prevention to increase by 1 to 5 percent next year, with 27 percent predicting an increase by more than 5 percent.

Funding is predicted to remain the same for 38 percent of organizations, and only 2 percent predict a decline.

To put these numbers in perspective, it is a very good year when 98 percent of organizations expect level-funded budgets or increases.

> It is a very good year when 98 percent of organizations expect level-funded budgets or increases.

If you expect a budget increase, where do you believe your organization will prioritize your spending?



For those organizations that predict a budget increase, 44 percent believe that awareness and training will receive additional funding, while 45 percent predict enhanced detection will be a priority.

Some 38 percent plan to spend more on endpoint security, and 36 percent plan to spend more on server security.

Deploying a network security solution also scores highly, with 39 percent predicting increases in spending in this area. The same percentage predict an uptick in spending on real-time endpoint or server monitoring.

© 2013 Information Security Media Group

2014 Cyber Security Agenda:
How to Put This Study to Work

In reviewing these survey results, several action items emerge for organizations to improve their ability to keep pace with advanced cyberthreats:

1 **Ignorance is Not an Option** – When 13 percent of respondent organizations do not know whether they have suffered a cyber attack in the past year, that's a problem. And it is symptomatic of the challenges organizations face detecting threats to endpoint devices and servers.

2 **Prioritize the Endpoint** – The vast majority of respondents say their greatest vulnerabilities are their users' endpoint devices. Yet, more than half say they are average at best when it comes to detecting suspicious activity on these devices. This is a deficiency organizations must address now – or else they will find out the hard way when the next cyber attack strikes.

3 **It's the Devil You Don't Know** – It's encouraging that 78 percent of respondents say their ability to defend against known, signature-based threats is average or very good. But many of today's advanced threats come without known signatures, and 66 percent of respondents rate their abilities here at average-to-non-existent. To be truly effective at detecting and preventing cyber attacks, organizations must become far better at spotting signature-less threats.

In his survey analysis, Bit9 CSO Nick Levay offered his key takeaways:

- First-generation security solutions cannot protect against today's sophisticated attackers.
- There is no silver bullet in security.
- There is an endpoint and server "blind spot."

In our next and final section, we feature excerpts of a Q&A with Nick Levay about what to look for in the next generation of security solutions.

© 2013 Information Security Media Group

Cyber Security Q&A with Bit9 CSO Nick Levay

NOTE: In compiling the 2013 Cyber Security Study Results webinar, Nick Levay, Bit9 CSO, answered questions about the survey and how security leaders can apply the findings. Following is an excerpt of Levay's insights.

Surprising Results

TOM FIELD: What if anything about the results came to you as a surprise?

NICK LEVAY: Well, I thought that 13 percent of respondents didn't know whether or not they had a serious cyber security event occur within their enterprise - I found that shocking. I would have expected that to be a single-digit number and a low single-digit number at that. One of the things that I think can be taken away from that is many organizations may not be tracking metrics regarding attacks as well as they should have because you typically know if you've responded to something. So, if you haven't responded to anything, that means you're certainly missing stuff.

Validation About Limitations

FIELD: What did you find to be particularly validating based on your own experience in the industry and your interactions with customers?

LEVAY: One of the things that I found validating about this survey was that 66 percent of respondents said that their organization's ability to protect themselves from signature-less threats was average, deficient, or nonexistent. That kind of tells me that a lot of people are waking up to the limitations of some of the solutions that they're using, and virtually all the other results said that they're actively looking for better ways to approach it.

I also saw that people seem to understand that there has been a progression in the security solutions available, and that what we were using the past five, 10 years, some of those technologies are going to start phasing themselves out and new things are coming in. And it seems like people are really looking for what those new things are. That's a good sign for security in general.

> A lot of people are waking up to the limitations of some of the solutions that they're using.

© 2013 Information Security Media Group

It's not just about blocking what's bad, it's not just about facilitating the type of activity that you want; it's also tracking and having a record of what happened.

Next-Gen Security

FIELD: I'd like to hear a little bit about what you envision as next-generation solutions. What are these solutions going to entail specifically?

LEVAY: One of the big things is visibility. A lot of the – and this is both on the endpoint and the network level solutions – visibility has become the big thing. In terms of networks, we were just simply trying to facilitate the network working. That's basically what everybody wanted. And the type of visibility that came back was usually just as simple as what we get from the most basic net flow, what's connecting to what at an IT level and over what ports. That's not enough. You've got to really see what the applications are and what the applications are doing.

And then on the endpoint, there's almost no visibility whatsoever traditionally. Even those antivirus solutions will only report back to their central management when they block something. They're not reporting back what they see running or what new software that they've seen come onto the system. And that's one of the things where the next-generation solutions like ours really differentiate themselves. We're not just telling you about the bad stuff that occurred; we're telling you all the high-value information about what's occurred on the endpoint. When a big piece of software comes in, you want that somewhere in your data set that you can drill into later from a response or forensics perspective.

So, that is one of the things that really kind of sets all the next-generation solutions apart. It's not just about blocking what's bad, it's not just about facilitating the type of activity that you want; it's also tracking and having a record of what happened.

What is the New Defense in Depth?

FIELD: In this next-generation context, how are we going to redefine what defense in depth means to an organization?

LEVAY: Well, I think when it comes to defense in depth, it's not so much that we're in a situation where we need to redefine what it means. I think we're in a situation where we need to simply rediscover what's an old concept.

I mean, there are some great truths that come across when you're doing security, and one of the biggest ones is that prevention eventually fails. No matter how elegant a solution is, no matter how well thought out it's implemented, at some point something is going to fail, be it based on human error, be it based on a technical flaw, it could be based on a gazillion things. But at some point any given defense is going to fail, and you need to anticipate that.

And one of the ways that you anticipate that is by layering defenses, and that is very traditional defense in depth. I mean, a good guideline that I always try to tell people when they're figuring out

© 2013 Information Security Media Group

> No matter how elegant a solution is, no matter how well thought out it's implemented, at some point something is going to fail.

or evaluating an attack or figuring out how they're going to defend themselves against a class of attack is that if you're depending on any one security control to solve an attack, you're doing it wrong. If you're looking at an analysis of an attack event, even one where the attack is blocked, if there wasn't another security control inline somewhere that couldn't stop that attack other than the one that actually did, you probably need to look at that and go, "Hmm, that's one area where we can advance our security staff. How can we make sure that this particular type of attack or class of attack we have another defense against it other than the one that actually stopped it?"

And, frankly, it's more fun to practice security that way. When you're looking at ways you can do what you're doing better, it's a little bit easier on the nerves than it is dealing with constant remediation and response to actual intrusion events.

Overcoming Blind Spots

FIELD: Now, you've talked about organizations' blind spots, based not just on our survey results, but what you see among your own customers. What are organizations missing?

LEVAY: Well, I'd put that into two categories. There's the data that you do not collect, and then there is the data that you collect but you do not use.

Now, in terms of the first category, data you don't collect, again, the endpoint is one of the places that most organizations are not collecting a lot of data. A lot of times they are; they're collecting data that isn't necessarily relevant. You're really trying to track what's going on on your endpoints – the Windows security event logs and stuff on the endpoints, that's not really what you're looking for. The specific data that you're looking for is usually how the system is changing, not just in terms of what application events are occurring, but what software is coming onto the system and what's it doing. That's one area where people aren't necessarily collecting the data in the first place.

But then the other problem is the data that you have that – or is at least accessible to you that you're either not collecting or not using well. And some of the things that I find shocking is a lot of organizations are collecting event logs having to do with authentication and whatnot. And the only thing that they're really bringing up and distilling and actually reporting on are authentication failures. I mean, you obviously want to know when authentication failures are occurring. But what about authentication successes? That's really the more important thing. What stuff is actually being resourced, or what stuff is actually being used and by whom? And ideally what for? And I find it amazing that a lot of organizations don't profile the actual usage of their network resources. They're just focusing on triaging whatever areas and alerts and bad stuff that's happening. ■

RESULTS WEBINAR

BANK INFO SECURITY®

The 2013 Cyber Security Study Results

Overview

Forty-seven percent of surveyed organizations have suffered a cyber attack in the past year. So, how equipped are global organizations to detect and defend against cyber attacks before they take root in endpoints and servers?

Register for the 2013 Cyber Security Study results webinar to learn more about:

- The impact of today's advanced cyber attacks;
- Where organizations are least prepared to detect and prevent advanced cyber attacks;
- Cyber attack defense spending priorities for 2014.

Presented by

Nick Levay

CSO, Bit9

Register Now

Become a Premium Member

Unlimited Webinars +
OnDemand Access
Learn more »

When it comes to

dbook BITS GRC Data Loss
y Theft Phishing Computer Security
irity Technology Vendor Interviews Bank
w Enforcement National Security Agency
gislation DIACAP ACH Fraud FISMA E-Go
yption ID & Ac ment Messaging
& Budget Hom Department En
raud Paymen aud Electroni
e Fraud Socia HITECH HIPA
pore Anti-Malv ngland Financi
Authority IBTRM DSCI Frameworks Adva
ation Education Incident Readiness Brea
fice Comptroller of Currency Office of Th
ecrecy Act ID Theft Phishing Emergi
ommission Privacy Risk Assessmen
-SIGN Act Sa -Oxley Act FAC
rnance Cobit O COSO PCAC
afety Privacy Security Mobile
t, Credit, Prepa iometrics Appli
efense Departn tors General In
ct Informatio mmittees and Tes
pplication Secu tion Biometrics
king Remote
hopping Frau
Audit Confiden
Management
t Act Check F
Network & Pe
partment End
Records HIE
CH Office of
ces Authority
rsistent Threat
se BYOD No
ion Federal F
Network/Peri
ement Social
Patriot Act In
C Handbook
entity Theft P
urity Technolo
Law Enforce
s Legislation
Loss Encrypt
Certifications Internet
Preparation Marketing How-To
ng Collaboration & Interagency Cong
et US-CERT Inspectors General C
aud Budgeting & Funding ATM Frau
Storage Web C2 Acad
ecurity Cloud SI
alized Medicine
Coordinator Office of Civ
Central Bank Data Protection
d Device Identification Log Ana
ntinuous Monitoring Payments P2
tional Credit Union Admininstra
rship & Management Ris
s SIM/SEM ID
IT Web Security
Data Loss obile Banking
Computer Security Phishing Shopping
ndor Interviews Banking Today Audit Cor
National Security Agency Office of
ACH Fraud FISMA E-Governm
Management Messag
uter Safety Or
heft Red Flags
ntracts Techn
Clinger-Coh
ecruitment A
Regulations &
ed Threat Man
ne Health and
tity Theft FHI A
Handbook ENISA APRA F
Forensics Threats & Vulnerab
Government Accountability Offic
nCEN AML/BSA Pharming Awa
gement Incident Response Informa
& Management mpliance NCUA
entication Base
Capture FISN
Pandemic Pre
n Banking Co
nt and Budget
ck Fraud Frau
twork & Perime
acy Wireless Sec
redit, Prepaid Car
se Department Ir
formation Sharin
n Security Auth
ves White Hous
ent Virtualizati
man Services C
Reserve Ban
n Security
ications Internet
arketing How-To
Interagency Co
nspectors Genera
Funding ATM
b Security ISC2

We've got you covered.

News | Education | Research

BANK INFO SECURITY®
US | UK | EU | IN | Asia

Just for Credit Unions
CU INFO SECURITY®

GOV INFO SECURITY®

HEALTHCARE INFO SECURITY®

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

CAREERS INFO SECURITY®
US | UK | EU | IN | Asia

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

iSMG
INFORMATION SECURITY MEDIA GROUP

www.ismgcorp.com