SURVEY RESULTS
REPORT

THE NEED FOR SPEED:

2013 Incident Response Survey

INSIDE

- Survey Results
- Analysis
- Expert Commentary

FireEye™

iSMG
INFORMATION SECURITY
MEDIA GROUP

From the Editor

Incident Response: Filling the Gaps

Survey Results Highlight Need for Greater Speed, Accuracy, Insight

Tom Field
VP Editorial, ISMG

Welcome to the 2013 Incident Response Survey report.

If I were to boil down these survey results to a single sentence, it would be this: To stay ahead of today's advanced threats, incident response teams need tools and techniques that give them greater speed, accuracy and insight.

It really is that fundamental.

As you'll see repeatedly in the pages ahead, under the shadow of today's advanced security threats, only 20 percent of organizations rate their incident response programs as "very effective." Their biggest gaps: Being able to detect and contain malware, which can also be the precursor to advanced persistent threats.

These are among the main takeaways from Information Security Media Group's 2013 Incident Response Survey, commissioned by FireEye. In this report and its companion webinar, you'll receive a comprehensive overview of survey results and expert analysis on:

- The top security threats for global organizations in 2013;
- Where the largest gaps exist in how organizations detect and respond to these threats;
- How these gaps will be filled in the coming year - by new staff, tools or services;
- What organizations must do to stay ahead of today's advanced threats.

In the end, yes, it does come down to the need for speed, accuracy and insight. How we get there is the trick, and we hope this report inspires some new ideas.

Please be sure to write to me with any reactions or comments about this survey report.

Best,

Tom Field
Vice President, Editorial
Information Security Media Group

Contents

The Need for Speed: 2013 Incident Response Survey

How Organizations Respond to Today's New Breed of Cyber Attacks

Sponsored by

FireEye™

FireEye® has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection 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 platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors, including Web, email, and files. 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 1,000 customers including over one-third of the Fortune 100.

Incident Response: A New Model Needed

The FireEye Perspective on Survey Findings

By Bill Hau, VP FireEye Labs

As I reviewed the survey results, two specific points struck me as most troubling. The first one is that only 20 percent of respondents rate their incident response program as being "very effective."

That leads me to worry about the other 80 percent. Is reasonably effective good enough? For those who responded "marginally" or "not at all" effective, how can they put an incident response program in place? The key point is making sure they are appropriately prepared to detect, contain and remediate the current advanced threats and attacks plaguing today's organization.

The second point that struck me was the notion of what we call "detection efficacy." And it comes from these three key survey statistics:

- **66 percent of respondents struggle to detect APT attacks in their environment.** What you can't see, you can't defend against. What this statistic suggests is that a larger part of our respondent audience is flying blind to what is happening within their organization.
- **62 percent struggle with the speed of detection.** The longer it takes to detect how and where the compromise took place, the longer attackers have to expand their footprint into environments and exfiltrate key information, significantly increasing the risk of damage.
- **44 percent struggle with the accuracy of detection.** Organizations that lack detection accuracy have limited visibility to confirm the stage, scope and exact locations of actual breaches. Compounding this problem is the sheer amount of data that must be mined through to determine what is real and what is not.

Bill Hau, VP FireEye Labs

Increased Risk

The survey results confirm the increasingly advanced nature of threats and the inability of current tools to detect them, which have increasingly plagued organizations and incident response teams over the past few years.

The pace of attacks has increased significantly. Based on the FireEye Advanced Threat Report, on average, a malware event occurs at a single organization once every three minutes. And the nature of these incidents has changed from broad, scattershot assaults to very targeted attacks, with persistent adversaries causing significant damage to organizations and individuals alike.

The volume of attacks has not only been increasing, as evidenced by the fact that 184 countries captured malware activity via callbacks over the past year - a 41 percent increase from 2010[1] - but they are also becoming more sophisticated. With an ever growing volume of readily available, sophisticated tools, the new generation of cyber-attackers create targeted, persistent and unknown threats, enabling them to evade traditional signature-based defenses, despite billions of dollars spent on these technologies. Firewalls, IPS, gateways or AV - it doesn't matter. They are all essentially defenseless in the face of these new attacks.

Shared Risk

As recent news headlines clearly show, everyone is at risk. Serious breaches have occurred consistently over the years to the best of firms, including some that invest millions in their security practices. According to the latest FireEye Advanced Threat Report, the attacks are across all verticals, but specifically targeting technology, financial services, manufacturing, healthcare and entertainment sectors.

1. Source: FireEye Advanced Cyber Attack Landscape Report

To put it simply, we need a new model that ensures incident response teams have access to timely, relevant and accurate information.

And we're not surprised that the survey results confirm that it's not just high profile companies in the headlines; it's everyone. The impact of these attacks has been equally alarming, with losses to intellectual property, compromised customer records and even destruction of data. And, what we are seeing and reading is only the tip of the iceberg.

Such breaches will continue to occur until appropriate technology and practices are put in place to allow incident response teams to quickly and accurately assess threats with insight into the entire life cycle of the attack.

Attackers: The New Generation

We have touched on the fact that the volume of attacks is increasing and that these attackers are becoming more and more sophisticated, but it's important to look at the technical reasons driving this change.

We discussed the coordinated threat actors and targeted nature of attacks. Additionally, threats are no longer the run-of-the-mill viruses and worms that ran amok 10 years ago. Attackers and their toolkits have gotten smarter, and evasion is a common practice, whether through multiple stages of attacks, multiple vectors or something as simple as polymorphism, which enables evasion of current security defenses by making simple changes to malware.

The incident response survey results show that not only are these attackers successful, but they are doing significant damage.

A New Security Model is Needed

It's obvious from the survey results that incident response teams are struggling with quickly and accurately detecting these attacks - if they detect them at all.

What can be done to address these gaps? To put it simply, we need a new model that ensures incident response teams have access to timely, relevant and accurate information, particularly given limited resources and high risks. Incident response teams need a way to cut through the noise and distinguish what is real and what is not. They need insight that allows them to balance timely detection with accuracy, and develop long-term threat awareness to effectively manage the next incident.

If incident response teams don't take these threats seriously and understand what they are up against, it's only a matter of time before – unfortunately – their organizations make the next headline.

Bill Hau is vice president of FireEye Labs. He has more than 15 years of experience as an information security practitioner, including CISO roles with finance and global consumer product businesses. He has hands-on incident response experience, including one of the largest 2012 security incidents.

Incident Response: Hot Topics

Data breaches – the types, quantity and cost – have been in the news of late and offer great context to the survey results we share in this report.

Verizon, for instance, recently released its annual Data Breach Investigations Report[1], analyzing 47,000 security incidents and 621 confirmed breaches. Among the relevant statistics:

- 92 percent of the breaches were perpetrated by outsiders;
- 40 percent incorporated malware;
- 66 percent took months or more to discover.

Similarly, Ponemon Institute and Symantec recently issued their global Cost of a Data Breach Analysis[2], and the findings include:

- The average cost of a data breach worldwide is now $136 per compromised record;
- 37 percent of incidents reviewed involved a malicious or criminal attack;
- Breaches resulting from malicious or criminal attack cost much more - $157 per compromised record.

With these findings in mind, let's turn to our own Incident Response Survey, commissioned by FireEye. This online survey was conducted by ISMG in the spring of 2013. Respondents include senior security and IT leaders from organizations of all sizes, primarily in the U.S. banking, healthcare and technology sectors.

Results show that respondents have heightened awareness to advanced security threats, but their current security defenses are failing to detect and respond appropriately to security incidents.

The hot topics that emerge from these results:

I. Costly Breaches

Malicious code, compromised devices and phishing attacks are compromising far more than system availability. Sensitive data, financial resources and corporate reputations also are at stake.

2. Ineffective Defenses

Sixty percent of survey respondents rate their current incident response programs as "reasonably effective." But when dealing with nation-state espionage, cyber crime, and advanced persistent threats, nothing short of "very effective" will suffice.

3. The Gaps

Current anti-malware tools are largely ineffective. Nearly half of survey respondents cannot determine the exact location of malware in their systems, and more than half cannot successfully define the extent of malware infiltration.

4. Incident Response Agenda

More than 90 percent of respondents expect stable budgets or increases. What are their key priorities for detecting, containing and mitigating advanced attacks?

1. Source: Verizon: 2013 Data Breach Investigations Report
2. Source: Ponemon Institute: 2013 Cost of Data Breach Study: Global Analysis

Costly Breaches

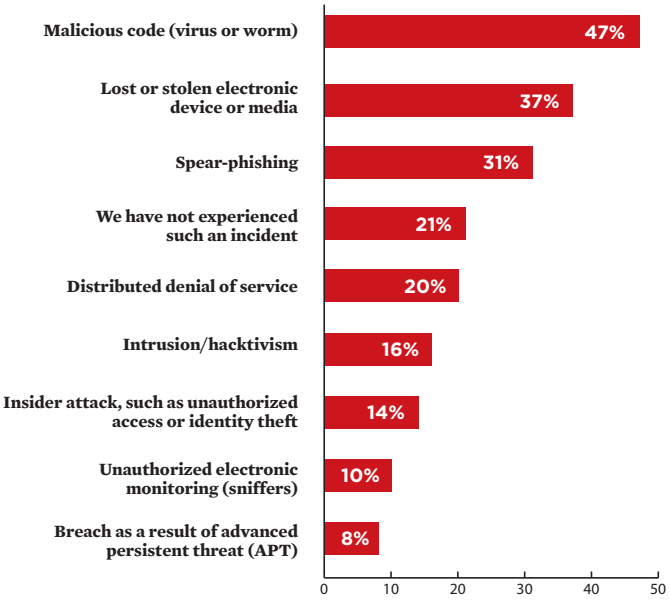
Note: In some instances the survey numbers do not add up to 100%. This is because A) Only the top responses are represented for space considerations, or B) The few unrepresented responses qualify as "other."

Some summary points to consider from our findings:

- Cybercrime and APTs are the primary security concerns;
- 47 percent of respondents were struck by malicious code in the past year – 31 percent were victims of spear-phishing;
- The cost: downtime, compromised data, and financial loss.

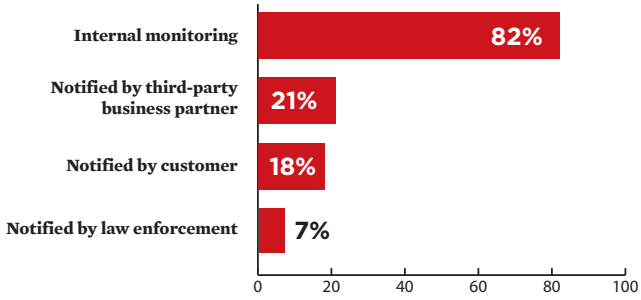
Key Findings:

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



The individual responses – malicious code, lost/stolen devices, spear-phishing, DDoS – are consistent with the news reports we've all seen, and they remind us that endpoint devices and servers are equal concerns for organizations. As you can see, 21 percent of respondents say they've experienced no such incidents in the past year. But based on what they later tell us about monitoring and detection, that estimate might be conservative.

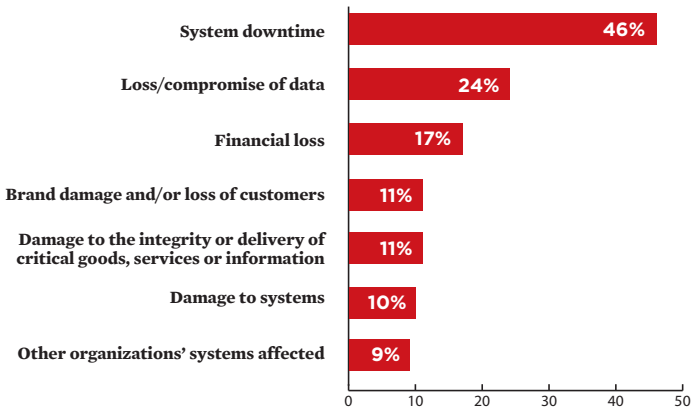
How did you detect the incident?



In the Verizon report, 69 percent of breaches were discovered by third-parties. In our survey, 82 percent of respondents say that at least some incidents were discovered by internal monitoring. But internal monitoring clearly is falling down when we learn this about incident detection:

- 21 percent of incidents were first noticed by third-party business partners;
- 18 percent were reported by customers;
- 7 percent were discovered by law enforcement.

What was the impact of the incident?



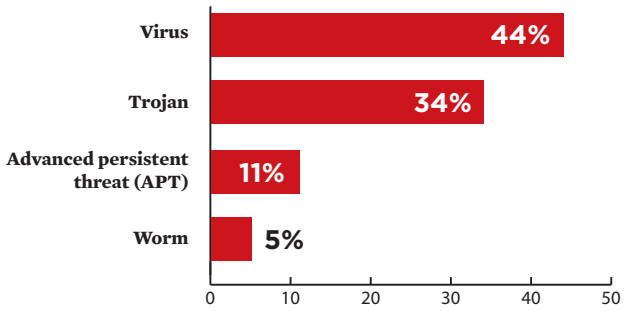
As noted in the Ponemon/Symantec Cost of a Data Breach report, damage runs the gamut of hard and soft costs – actual damage to systems or financial loss vs. reputational damage and loss of customers.

System downtime, data loss and financial loss are the top three impacts of security incidents, according to our survey. But don't minimize the lesser-reported effects, including brand damage.

The repercussions are frightening, and some organizations never recover from them.

So, given the impact of intrusions, let's see what's penetrating these organizations.

Which are the most common forms of malware detected by your organization?

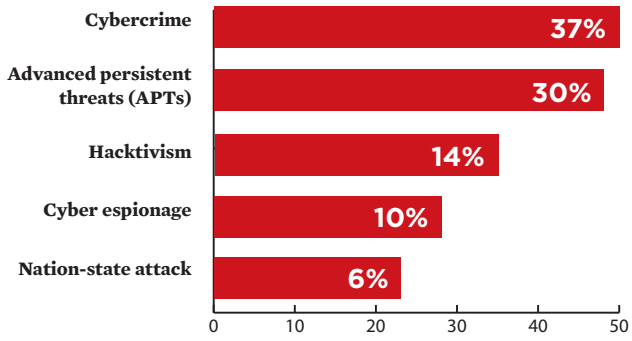


We hear so much these days about malware and especially the Trojans – Zeus, SpyEye, and Citadel – and how they permeate networks in search of account information and the ingredients of identity theft.

So it's no surprise that our respondents are predominantly experiencing viruses and Trojans. The only additional point to consider: This finding represents what the organizations have detected. What have they not detected?

Cybercrime and advanced persistent threats – these are the attacks organizations fear most.

What do you perceive as your greatest cyberthreat?



Cybercrime and advanced persistent threats – these are the attacks organizations fear most.

We live and work in an age of cybercrime and hacktivism, where fraudsters want to plunder your accounts; protesters want to embarrass you for ideological means; and perhaps nation-states and competitors seek to extract competitive data. The answers to this question reflect the news we read daily about risks, threats and breaches.

But now, as we transition into our section about organizations' defenses, the question we want to take with us is: How well are organizations prepared to respond to cybercrime and APT?

Expert Analysis: Today's Top Threats

By Bill Hau, VP FireEye Labs

According to our customers, advanced malware is where the fear factor is greatest. This type of malware is so complex and able to evade traditional signature-based defenses, and typically comes in through multiple vectors, including Web, email and file shares.

Once in your environment, the advanced malware proceeds to set up a command-and-control channel, where it communicates outbound to its handlers. These handlers then download additional malware to elevate their privileges or perform other invasive activities. They could be seeking intellectual property or "trojanizing" your existing software, such as your word processor, software updaters etc., for additional outbound communication mechanisms to the handlers. Once they have found any information of interest, they will create a bypass around any data loss prevention technology currently in place.

And perhaps most damaging is, once the malicious actors have determined they have everything they need, they often sell or trade the compromised assets to criminal groups and they can come back in to exfiltrate additional information from that network. Clearly, there is good reason why organizations should be concerned about this type of attack.

Ineffective Defenses

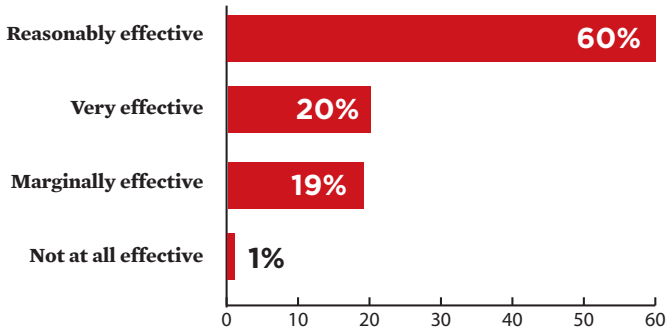
As we look at respondent organizations' defenses, we already have one salient fact: Only 20 percent of respondents believe their organizations' incident response programs are "very effective."

Here are some other summary findings:

- Only 26 percent of respondents rate anti-malware tools "very effective;"
- 44 percent struggle to determine the exact location of malware;
- 56 percent are challenged to determine the extent of malware infiltration.

Key Findings:

How would you rate the current effectiveness of your incident response program?



At first glance, you might think 60 percent say their programs are reasonably effective – that's pretty good.

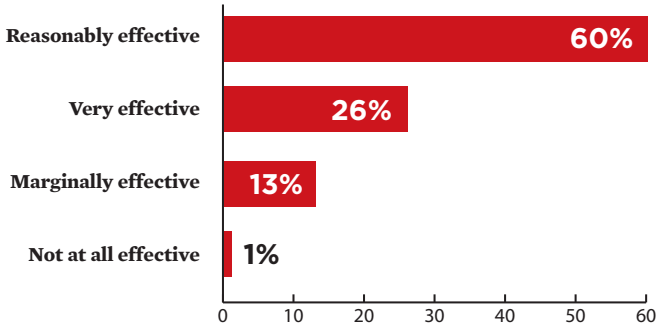
But is "reasonably effective" going to ward off advanced attacks? Is it going to satisfy a regulatory examiner, a breached customer or your own board of directors?

If you represent a government agency, do you want to sit before a congressional committee and describe the meaning of "reasonably effective?"

Is "reasonably effective" going to ward off advanced attacks? Is it going to satisfy a regulatory examiner, a breached customer or your own board of directors?

Again, given some other survey responses, one wonders whether the 20 percent who describe their programs as "very effective" aren't offering an overly-optimistic view. Let's review some other responses.

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



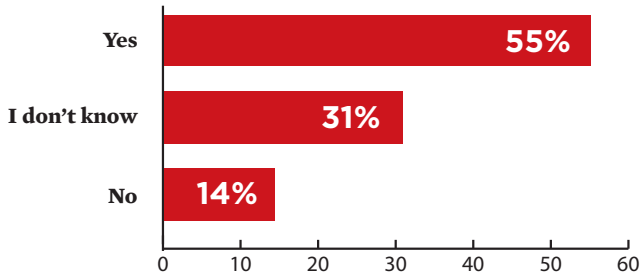
First, a bit of context. We also asked respondents, "Which anti-malware tools does your organization currently use?" Nearly 90 percent say they are using some kind of commercial anti-malware solution.

How effective are these commercial tools? Once more, we see 60 percent of respondents who rate their tools as "reasonably effective." But we already have dissected the potential meaning of those words.

A smaller number, but bigger issue: When only 26 percent of respondents describe the tools as "very effective" ... that's one significant source of intrusion. The tools are not good enough to ward off the attackers.

Next, let's review responses to questions about detection.

Can you detect the exact location of malware in your environment?

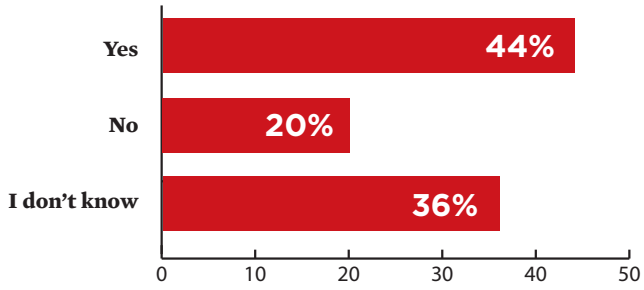


The 14 percent of respondents who say they cannot detect the exact location of malware are not as big of a concern as the 31 percent that do not know.

Remember the Verizon statistics about 69 percent of breaches being discovered by third parties, and 66 percent taking months or more to discover? This is one of the reasons why: Pure inability to detect.

The next logical question:

Can you currently determine the extent and/or stage of malware infiltration or propagation?



This response speaks directly to a distinct lack of real-time visibility into endpoints and servers and how they are being compromised by advanced attacks. How can an incident response team determine the extent of damage if it does not have appropriate and timely visibility into infected systems?

Go back to the earlier question about "What do you perceive as your greatest cyberthreat?" One of the two top answers – and by a wide margin – is "Advanced Persistent Threat."

One would think that current incident response programs would reflect that concern. But survey responses say otherwise.

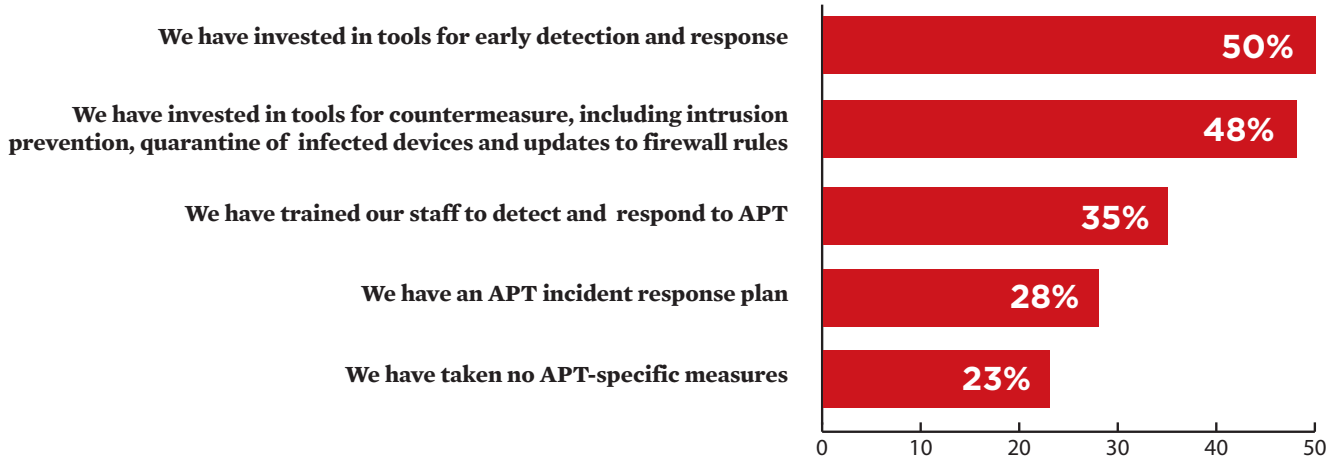
Half of respondents have invested in tools for early detection and response (although this survey would suggest that organizations have yet to see a significant payoff). And nearly half have invested in tools for counter-measures, i.e. intrusion prevention, quarantine of infected devices, etc.

But less than one-third have an actual APT incident response plan.

And nearly one-quarter say: "We have taken no APT-specific measures."

As the name of this section suggests, current defenses are ineffective. In our next section, we'll explore how these inadequacies create significant security gaps.

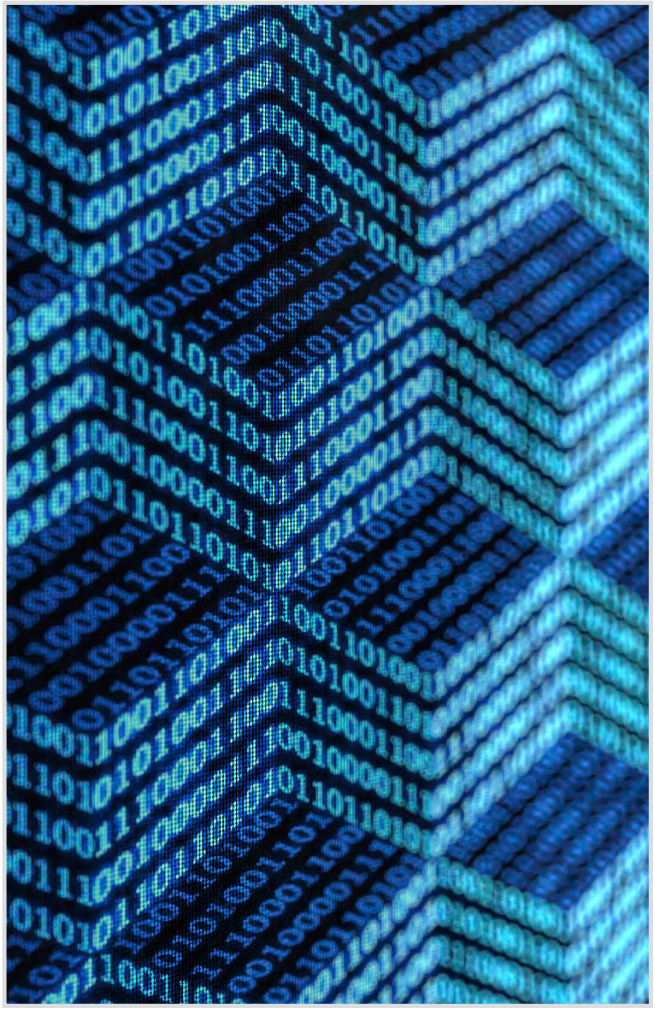
How is your organization prepared to respond to advanced persistent threats?



Expert Analysis: How Effective is 'Reasonably Effective?'

By Bill Hau, VP FireEye Labs

In the survey analysis, we've emphasized the fact that only 20 percent of respondents rate their incident response programs as "very effective."



Sixty percent rate their programs as "reasonably effective," which begs the question: What is reasonable?

I look at the statement this way: "What if I had reasonably effective brakes on my car?"

The real answer to "what is reasonable?" is best determined on a case-by-case basis. When a breach occurs - and you know it's occurred - the proof will be when you dust off your incident response plan and start to follow it.

The key priority for these "reasonably effective" programs is to make sure they have performed a risk assessment to ensure their incident response program addresses the right kind of protection against their threat scenario. They must make sure they are protecting against the advanced threats they may encounter in their environment and build a foundation around those scenarios.

The real answer to "what is reasonable?" is best determined on a case-by-case basis.

The Gaps

We asked respondents to self-assess their top security and technical challenges that influenced incident response. Here are the summary findings:

Top Security Challenges:

- Speed of detection
- Accuracy of detection
- Monitoring

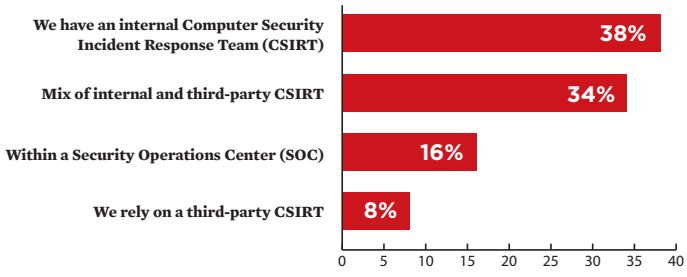
Top Technical Challenges:

- Real-time detection
- Effective response
- Lack of skills

Key Findings:

For context, it helps to understand how an incident response team is organized.

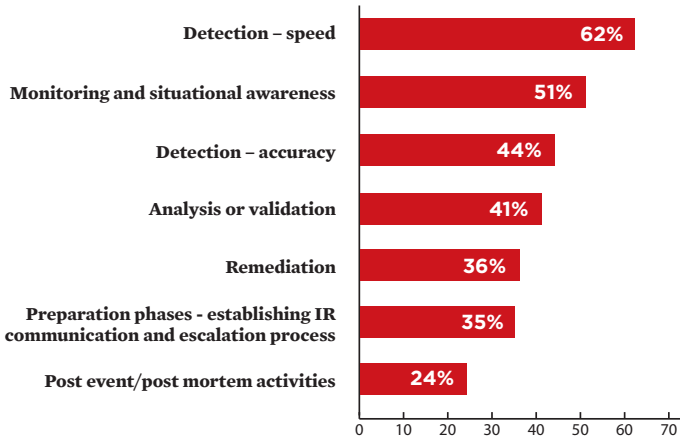
How is your incident response team organized?



Respondents here hit on the operative words of this study – the lack of timeliness, accuracy and insight.

Next, we look at specific challenges, which start to reveal the gaps foreshadowed earlier in this report.

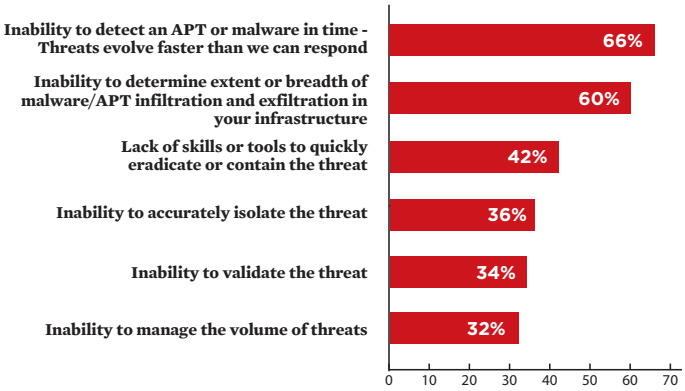
What do you believe are the top 3 security challenges in your IR cycle?



Respondents here really hit on the operative words of this study – the lack of speed, accuracy and insight from their current incident response processes.

Next, let's review technical challenges.

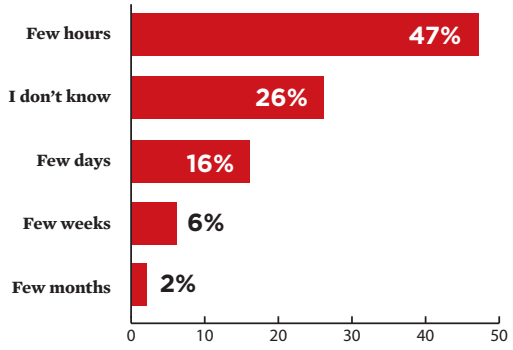
What do you believe are the top 3 technical challenges that impact the ability for effective incident response?



As you see, the technical challenges really come down to visibility into systems and the ability to detect in real-time what's coming at the endpoints and servers – and the extent of the damage.

So, lacking fast, accurate detection, how do organizations assess their abilities to respond to incidents? Here are two barometers:

From early indicator of compromise to actual detection, what is your organization's mean time to discovery?



Expert Analysis: Reducing Detection and Response Times

By Bill Hau, VP FireEye Labs

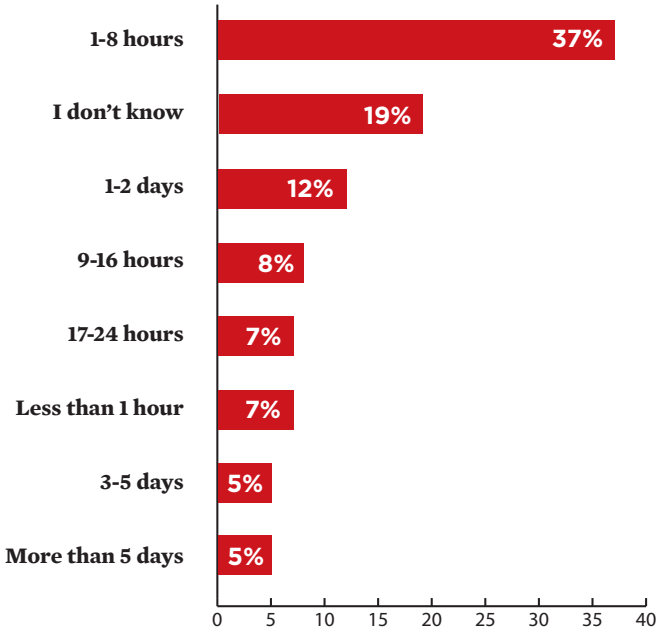
As Verizon's 2013 DBIR report suggests, and our survey findings reveal, it can take weeks or even months for organizations to detect advanced threats within their organizations.

Obviously, these times must be reduced.

FireEye technology provides organizations with a purpose-built, virtual machine-based security platform that provides real-time threat protection against the next generation of cyber attacks. FireEye can take discovery and response times down from weeks or months to minutes. And if an advanced attack can be detected within minutes, the exposure for organizations is reduced significantly, allowing less time for proliferation of the attack and exfiltration of assets.

FireEye technology also provides accurate alerts that incident response teams need to remove false positives and false negatives, which hinder the process and waste valuable resource time. Organizations can quickly confirm malware location, depth and criticality with enough precision to isolate attacks, prevent further damage, and trigger only the necessary remediation actions. With timely detection and accurate alerts, incident response teams gain real-time insight to make intelligent trade-offs between malware risk and business up-time while also planning defenses against future attacks.

Following security incident detection, what is your organization's mean time to resolution (MTTR)?



Let's go back to the Verizon survey and one of its most telling data points: 66 percent of breaches took months or more to discover.

Given that context, and seeing that our respondent organizations struggle to detect breaches, it seems optimistic that the mean time to discovery is primarily hours, or MTTR is contained within a single business day.

A little easier to accept, frankly, is that more than 25 percent of respondents don't know their discovery time, and nearly 20 percent are unaware of MTTR.

It is more than fair to say, gauging the resonant themes throughout these survey results, that respondent organizations have huge gaps in how they monitor their systems, how they accurately detect malware infections, and then how they act on threat intelligence effectively.

In our final Hot Topic, we review strategies to fill these gaps.

Incident Response Agenda

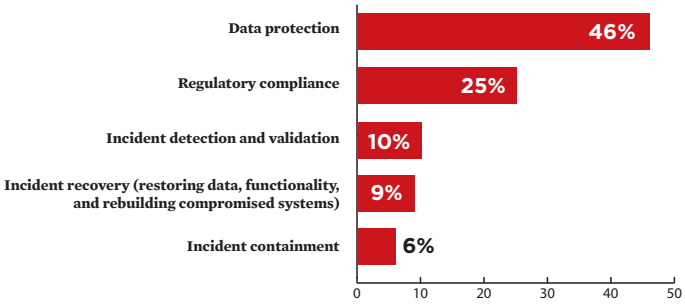
The encouraging news for the coming year:

- 42 percent of respondents expect their incident response budget to increase;
- Top spending priorities: Training and automated tools for incident detection and containment.

Key Findings:

We start by identifying organizations' top incident response priorities for the coming year.

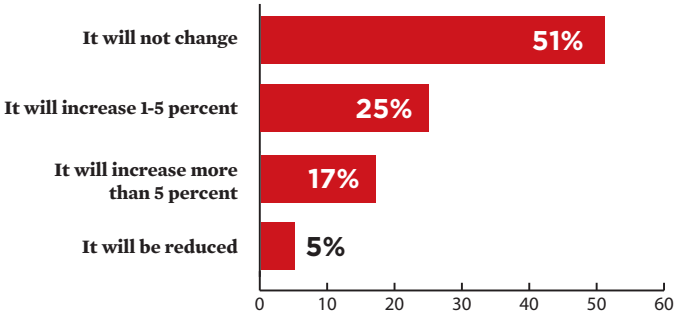
What do you identify as your greatest priority?



No shocking news here – we've already uncovered the greatest vulnerabilities, and we know what organizations need to do maintain business continuity and brand. They have to protect the data – particularly if they are regulated entities such as banks, healthcare organizations and government agencies.

But how are they going to meet these objectives?

How will your incident response budget change in 2013?



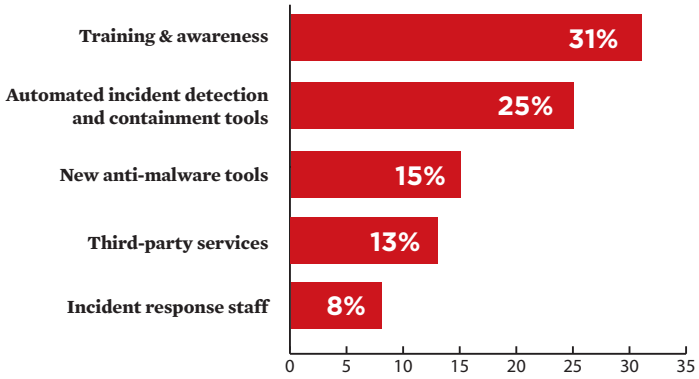
Organizations are going to spend. Noting only 5 percent of respondents reporting incident response budget decreases is encouraging news. More than 90 percent expect at worst to be level-funded. At best they will see budget increases of more than 5 percent. This is good news in any economy, never mind coming out of the hard times many organizations experienced in recent years.

And, frankly, it's the worst news we've given yet to potential attackers.

Asked how they will spend their money, respondents identify two clear priorities:

How are organizations going to meet their objectives? They are going to spend.

What will be your top spending priority in 2013?



Automated tools represent a great starting point. Organizations are largely missing the boat when it comes to real-time detection and response – they need far greater visibility into intrusions and infiltrations. Then they need to be able to see and respond immediately to alerts of anomalous activity. There are tools out there that can reduce their detection and response times dramatically.

Training/awareness could go one of two ways. On one hand, organizations can go far by doing a better job of deputizing their own employees to be more vigilant about basic security practices: Keep their anti-malware current; don't click on suspicious links; report any activity that strikes them as suspicious.

But on the other hand, training/awareness is also one of those areas that organizations traditionally pay lip-service to, but do not follow through with well. While not specifically addressed in this survey, we see a consistent thread in other studies: Security awareness/training at far too many organizations is often a one-time event.

That has to change for any of the incident response best practices to truly take root.

So, where do we go from here?

Incident Response Agenda: It's About Speed, Accuracy, Insight

We have demonstrated why only 20 percent of organizations believe their incident response programs are "very effective."

To improve that number, security leaders and IR professionals must embrace three key words:

- **Speed** – They must strive to take the unknowns out of detection. When systems have been breached, you need to rely on real-time detection, response, and containment. Not just the tools, but also the trained personnel.

- **Accuracy** – Know and respond to the true extent of infiltration. To be accurate, you need better analytics to know when malware has hit your systems and exactly how extensive the potential damage is.

- **Insight** – To paraphrase a pop culture quote, with great insight comes great responsibility. When organizations have the proper tools and trained staff to monitor systems and detect advanced attacks, then they must use those resources to improve response, containment and remediation times. Prevention is the ideal – resolve the incidents before they occur. But when you can't ward off the attack, at least be prepared to limit the damage.

When organizations have the proper tools and trained staff to monitor systems and detect advanced attacks, then they must use those resources to improve response, containment and remediation times.


WEBINAR
The Need for Speed:
2013 Incident Response
Survey Results
How Organizations Can Respond Faster to
Today's New Breed of Cyber-Attacks
• The top security threats for global organizations in 2013;
• Where the largest gaps exist and how organizations detect and respond to these threats;
• How these gaps will be filled in the coming year - by new staff, tools and services;
• What organizations must do to stay ahead of these advanced threats.
Register Now
http://www.inforisktoday.com/webinars/need-for-speed-2013-incident-response-survey-results-w-350
FireEye