CYBER SECURITY INCIDENT RESPONSE:

Are we as prepared as we think?

Sponsored by Lancope

Independently conducted by Ponemon Institute LLC

Publication Date: January 2014

Ponemon INSTITUTE

Table of Contents

Executive Summary

THERE IS NO QUESTION that organizations of all sizes face a significant threat from information security breaches. Cyber-attacks have become more commonplace and more sophisticated with each passing year. There are a variety of challenges that today's security organizations have to deal with, including:

- malware campaigns launched by organized criminal groups who look to steal information that can be sold on the black market
- increasingly powerful distributed denial-of-service (DDoS) attacks that can take out large websites
- state-sponsored espionage that can penetrate even well-defended networks.

Organizations need to be prepared to respond when these incidents happen. A Computer Security Incident Response Team (CSIRT) is a team of security experts within an organization whose main focus is to respond to computer security incidents, provide the necessary services to handle them and support the organization to quickly recover from security breaches.

In this study, we surveyed 674 IT and IT security professionals in the United States (n=357) and the United Kingdom (n=317) in order to determine the level of preparedness of their Computer Security Incident Response Teams. To ensure knowledgeable responses, all participants in this research have some level of familiarity and involvement with their organization's CSIRT activities.

In the past 24 months, most organizations represented in this study had at least one security incident[1] and expect that another incident will occur in the near future. **Most respondents agreed that the best thing that their organizations could do to mitigate future breaches is to improve their incident response capabilities.** This recommendation was more popular than preventative security measures such as vulnerability audits and end-user education efforts.

57%

of respondents expect to experience a security breach within the next year.

In spite of these facts, **most survey respondents indicate that investment in incident response capabilities in their organization has remained static over the past 24 months relative to other IT security expenditures.** In fact, 34 percent indicated that their organizations do not have a fully functional CSIRT at all, and many CSIRTS that do exist lack full-time staff. This is particularly alarming considering that nearly half of the respondents anticipate another breach within the next six months, and that it takes an average of at least one month to resolve each incident.

Only 20%

of respondents regularly communicate with management about threats.

Another key observation is that C-Suite executives are often not informed about CSIRT activities. **Only 20 percent of respondents say they very frequently or frequently communicate with executive management about potential cyber-attacks or threats against the organization.**

1 Incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies or standard security practices.

Further, only 14 percent say executive management takes part in the incident response process. As a consequence of this lack of involvement and awareness, CSIRTs may find it difficult to obtain the resources from leadership to invest in the expertise and technologies necessary to deal with future security incidents.

Today's IT security teams must be squarely focused on business continuity, not just on catching crooks. In the information age, security incident response should be a regular and prominent part of doing business, versus just a siloed effort relegated to the IT team.

1 month

The amount of time survey respondents say it took to investigate, restore service, and verify resolution of incidents.

Following are some of the most salient findings from this research:

Investment is critical for effective cyber incident response programs.

- Sixty-eight percent of respondents say that their organization experienced a security breach or incident in the past 24 months. Forty-six percent say another incident is imminent and could happen within the next six months.
- Eighty-one percent believe that if the right investments in people, process and technologies were in place, their organizations would be better able to mitigate all future security breaches. Respondents indicated that better incident response capabilities as well as threat intelligence and IP reputation services would most help mitigate future security breaches.
- However, most respondents say that less than 10 percent of their security budget is used for incident response activities, and this percentage has not increased over the past 24 months.
- In fact, 34 percent indicated that their organizations do not have a fully functional CSIRT.

Metrics can help determine CSIRT effectiveness.

- Fifty percent of respondents say their organization does not have meaningful operational metrics to measure the overall effectiveness of incident response activities.
- Knowing is not half the battle: Although respondents say that they can identify security incidents within hours, it takes about a month to work through the entire process of incident investigation, service restoration and verification.

CSIRTs are ill-prepared to respond to cyber threats.

- Forty-seven percent of respondents either do not assess the readiness of their incident response teams or do not do so regularly.
- Only 23 percent of respondents indicated that their organization has a predefined public relations and analyst relations plan in place that can be activated in the event of a material breach that needs to be publicly disclosed.
- Most organizations aren't sharing threat information. Forty-five percent of respondents indicated that they do not share or receive threat intelligence and threat indicator information from other organizations. Another 26 percent indicated that they receive information but they do not share it.

Network audit trails are the most effective tool for incident response.

- Eighty percent of respondents indicated that analysis of audit trails from sources like NetFlow and packet captures was the most effective approach for detecting security incidents and breaches.
- This choice was more popular than intrusion detection systems and anti-virus software.

Management is largely unaware of cyber security threats.

- Only 20 percent of respondents say that they frequently communicate with executive management about potential cyber-attacks or threats against the organization.
- Only 14 percent say executive management takes part in the incident response process.

Background on the Cyber Security Threat Landscape

OVER THE PAST 10 years, most organizations have made improvements in their approach to computer security. They've hired teams of people to perform vulnerability assessments and comply with best practices. They've deployed increasingly advanced technologies to protect their networks. They've educated their employees about dangerous behaviors. On the whole, most companies are better prepared for cyber-attacks now than they have ever been.

In spite of all this effort and expense, computer security remains an unsolved problem. At the same time that most organizations have gotten better at defending themselves, attackers have gotten more sophisticated. The amount of economic opportunity that computer network attacks represent has continued to increase, and that has attracted more criminal groups and motivated them to find ways to subvert companies' defenses.

As attacks have become more sophisticated, the need for Computer Security Incident Response Teams (CSIRTs) has grown. This is not merely because attacks are still successful. It is also because the kinds of attacks people are facing can often only be stopped with human intervention. There are four categories of attack that are worth considering in this light:

- Botnets
- Distributed denial-of-service (DDoS) attacks
- Insider threats
- Advanced persistent threats (APTs).

Botnets

Botnet operators are usually financially motivated – they assemble large networks of infected hosts that they use to harvest login credentials and financial information, or launch DDoS attacks. We often rely on automated tools such as anti-virus and intrusion prevention systems to detect and block the exploits and malware associated with botnet propagation, but these tools are not always effective.

Botnet operators have demonstrated that they can generate new samples that can evade detection, so most organizations are still struggling with infected hosts even if they have good technologies and practices in place. Responding to these infected hosts and cleaning them up is the most basic capability of an incident response team, and it will be needed until botnet operators find that they can no longer evade automated detection solutions.

DDoS

The volume of DDoS attacks on the Internet has increased dramatically in the past few years. So has the amount of traffic that attackers can generate during an attack. These attacks have become popular with political extremists who wish to disable Internet services in order to make a statement, and they are also used by organized criminals to blackmail companies as well as distract their incident responders while other targeted attacks are launched at the same time.

In the past few years, a new market has emerged for DDoS service providers that offer to take down web sites for a price. These service providers compete with each other by developing new techniques for generating large amounts of traffic and evading automated systems that are used to protect networks from attack. Because DDoS attacks can be multifaceted and unpredictable, organizations that face them need human incident responders who can monitor the attacks and engage in appropriate mitigations in real time.

Insider Threats

The insider threat is often authorized to get past an organization's security controls because he or she has access to the data that will be stolen in the course of his or her job. The best way to detect a rogue employee isn't usually a software security system. It's the keen eye of a manager who realizes that an employee is disgruntled and may be capable of taking things too far, or the coworker who overhears a threat being made toward the organization. These human observations can lead to investigations that examine computer systems and networks, but that's only possible if an incident response team is available and has access to the right logs and audit trails.

Advanced Persistent Threats (APTs)

The class of adversary that is having the biggest impact on incident response teams is the Advanced Persistent Threat. The Internet is increasingly becoming a theater in which international conflict and espionage between nation states is taking place, and a growing cross-section of organizations are finding themselves in the line of fire. Sophisticated attackers are able to evade automated defenses, and they may have a long-term, strategic interest in compromising an organization and collecting information from it. As these attacks are often targeted, the tactics that one organization experiences may differ from what other organizations are seeing.

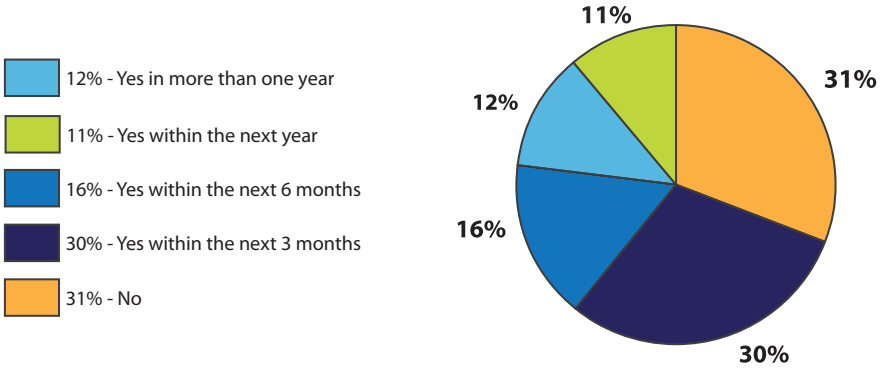
In this domain, the importance of a well-equipped, in-house incident response team is vital, as defense is not just a matter of cleaning up infected computers after the fact, but of fully dissecting and understanding the attacks that are taking place, and applying that understanding to protecting the organization against future attacks. Although super computers can be programmed to play chess, when faced with a strategic, targeted attack on your computer network, you're going to want a human playing for your side.

The Current State of Computer Security Incident Response Teams

Organizations that face cyber-attacks need to be prepared to respond to them.

Most of the organizations represented in this study (68 percent) had a security breach or incident in the past 24 months, and 46 percent say another incident is imminent and could happen within the next six months. Furthermore, more than a third of respondents (34 percent) said they did not have a fully functional CSIRT in place today to respond to those incidents when they occur.

FIGURE 1. Do you anticipate that your organization will experience a material security breach sometime in the near future?



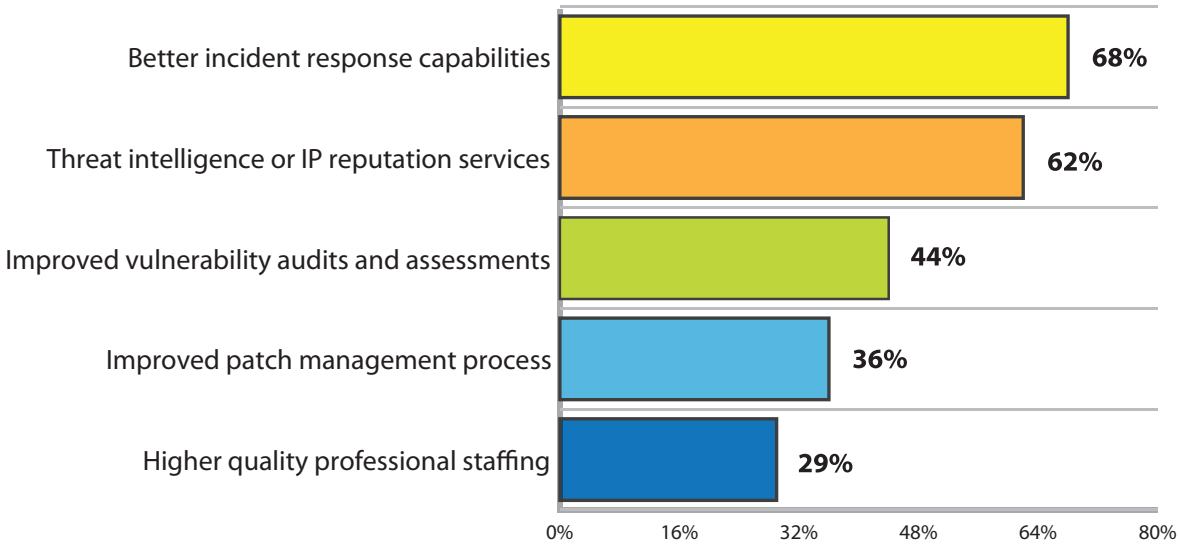
There was widespread agreement among survey respondents that investments in incident response capabilities are worthwhile.

Eighty-one percent of respondents agreed that the right investments in people, process and technologies would allow their organization to mitigate all future security breaches. This is a very high percentage given the technical and operational challenges associated with protecting organizations against cyber-attacks.

When asked what improvements would help their organization best mitigate future security breaches, the most popular answer was better incident response capabilities, at 68 percent, followed closely by threat intelligence and IP reputation services. It is noteworthy that these choices were more popular than common preventative measures such as vulnerability audits and patch management.

FIGURE 2. Most effective practices for mitigating future security breaches

Three responses permitted

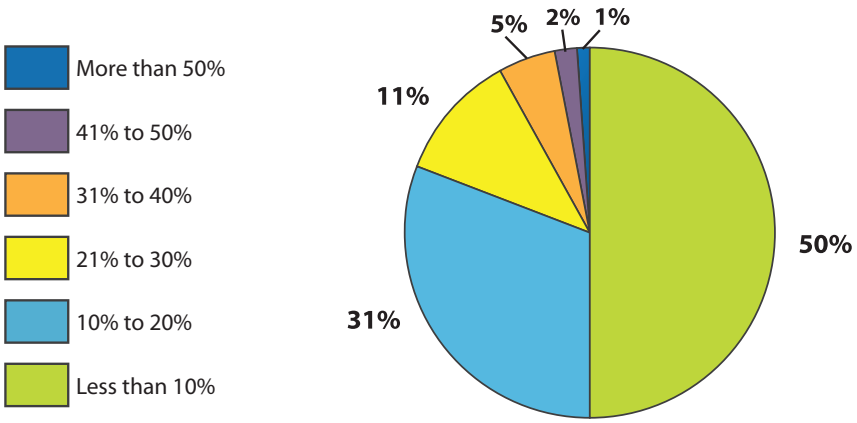


There appears to be a disconnect between the perceived value of incident response teams and the amount of money being invested in them.

Although our survey respondents agree that more investment in incident response is needed, they are not seeing that change happen in their organizations. Only 34 percent of respondents indicated that the budget allocated for incident response personnel, tools and technologies has increased over the past 24 months as a percentage of the overall security budget. Half of the respondents indicated that spending on incident response capabilities was less than 10 percent of their overall information security budget.

FIGURE 3. What percentage of your organization's security budget is allocated to incident response?

Please include personnel, services and technology costs/investments in your estimate.



Why aren't organizations investing more in incident response?

ONE POSSIBLE EXPLANATION is that incident response investments are viewed as reactive rather than preventative. Ideally, breaches would not occur, and therefore there would be no need for teams to respond to them. With a limited budget for protecting an organization against security problems, it may be easier to rationalize spending that money on measures that are designed to stop breaches from occurring in the first place rather than on measures that are designed to respond to a breach once it has happened.

However, incident response teams don't merely clean up security breaches; they seek to understand them. Part of the process of responding to a security incident is to establish its scope by identifying the systems and networks that were compromised and the datasets that were exposed. In order to perform this analysis, the incident responder must reconstruct the steps that the attacker has taken, as much as possible. Through this process of following in the attacker's footsteps, a clear picture emerges of where the attacker came from, how they broke in, and what they were after.

This information can be vital to an organization that needs to prioritize preventative investments. Those investments can be focused on the specific deficiencies and vulnerabilities that attackers are targeting in practice. Furthermore, specific knowledge of the attackers that are targeting the organization can be helpful in monitoring for future attacks.

This may be why threat intelligence and IP reputation services ranked a close second in our survey, after incident response capabilities, as the best way that organizations can mitigate future breaches. The next best thing to knowing more about the attackers that are targeting your organization is knowing more about the attackers that are targeting your peers.

The Makeup of Computer Security Incident Response Teams

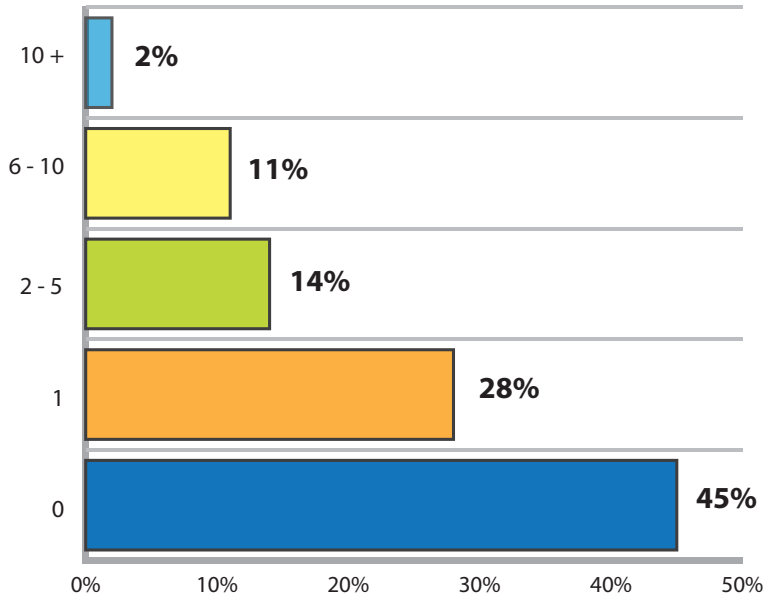
CSIRT programs are made up of experienced and credentialed experts, but lack full-time staff.

Of the respondents who say their organization has a CSIRT, most of those CSIRTs have been in place for at least three years. CSIRTs usually have several employees assigned to them. However, these employees split time between supporting CSIRT activities and other job responsibilities. Forty-five percent indicated that their CSIRT had no full-time staff at all, and only 27 percent had more than one full-time employee.

According to the survey, many CSIRT members have more than 10 years of relevant experience (54 percent of respondents) and most have security credentials (CISSP, CISM, CISA and others). However, less than half of respondents say CSIRT members in their organization undergo specialized training on an ongoing basis.

FIGURE 4. How many team members are fully dedicated to CSIRT?

Three responses permitted

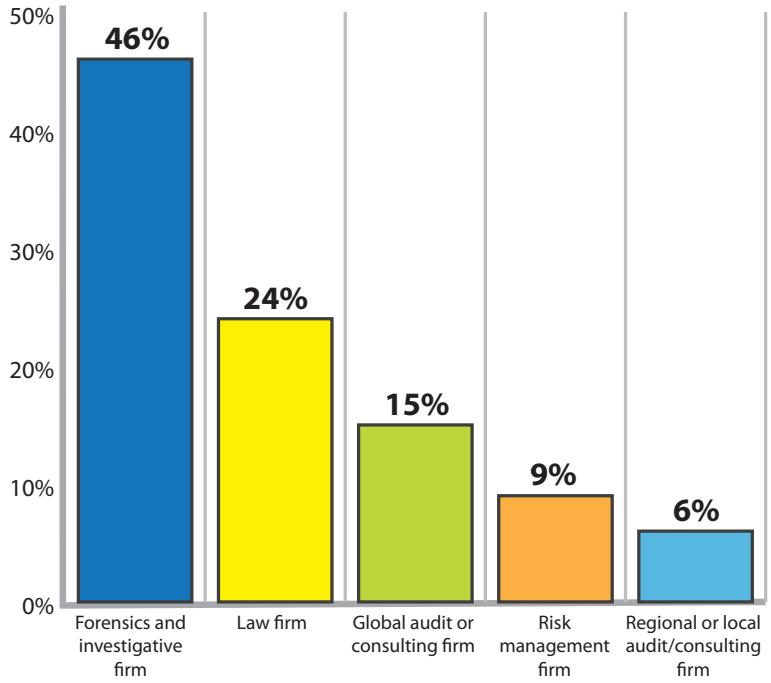


Most organizations keep incident response in-house.

Only 35 percent of respondents say their organization has a retainer or master service agreement with a third-party consulting firm that assists with incident response. Most often, these firms are used to augment the skill set and capacity of the in-house team, rather than serving as a substitute.

FIGURE 5. Third-party service provider selected in the event of an incident?

Three responses permitted



Why retain consultants?

THIRD-PARTY CONSULTANTS are not a perfect substitute for having in-house staff responsible for incident response. In order to respond to an incident rapidly, an incident response team must have an understanding of the IT infrastructure they are investigating as well as the business running on top of it.

A third-party contractor can lose precious time navigating to the resources they need. In addition, many of the tools and audit trails that are needed in order to respond effectively to an incident must be in place before the incident begins, and cannot be established on the fly during an incident.

However, the use of outside consultants to augment the capacity of in-house staff is a best practice that is often recommended by incident response professionals. Responding to a significant breach is not a 9-to-5 endeavor. A breach could be discovered at any time of the day, and incident responders may be working around the clock for several days to determine the scope of the breach and bring it under control.

People who are working long hours while trying to unravel a complicated technical problem in the midst of a crisis may be prone to making mistakes. It is better to enable employees to work in shifts so that analysts can get some sleep while the incident continues to be investigated. According to Figure 5, the third-party services most often used are forensics and investigations followed by legal and auditing.

Measuring Incident Response Effectiveness

THE MOST MATURE organizations not only have a CSIRT in place, they also have meaningful operational metrics that they can use to assess whether that CSIRT is able to respond to incidents effectively. Keeping track of security incidents is not just necessary in order to understand and measure the incident response team, it is necessary in order to understand the overall security posture of the organization.

Most information security programs ultimately boil down to making investments that reduce the number of incidents the organization is experiencing and the impact that those incidents have on the business. The time and effort required to identify, respond to and resolve each incident are important components of the overall cost of that incident to the organization. Therefore, without a quantifiable understanding of incident response, it is impossible to accurately measure the return on investment of any information security project.

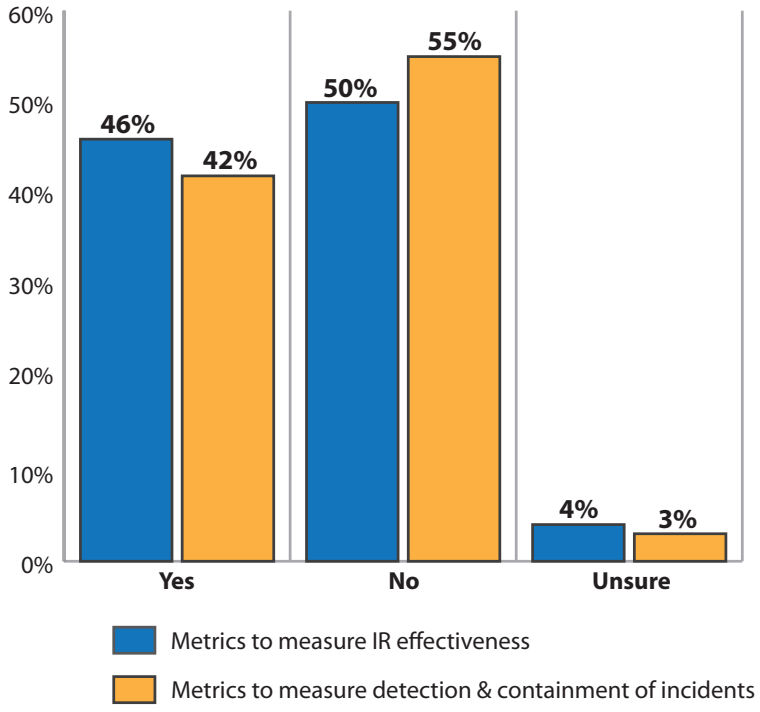
Unfortunately, most of the organizations we surveyed have no way to measure the effectiveness of their incident response teams.

Figure 6 reveals that the majority of organizations are not keeping track of the speed at which incidents are detected and contained, nor the overall effectiveness of their incident response process. As a consequence, management is often in the dark about the organization's ability to respond to incidents and perhaps about the return on investment associated with information security in general.

This lack of evidence contributes to the siloed nature of IT security in many organizations. In this day and age, cyber security really needs to be a core part of the overall strategy for business continuity.

FIGURE 6. Use of operational metrics

Three responses permitted



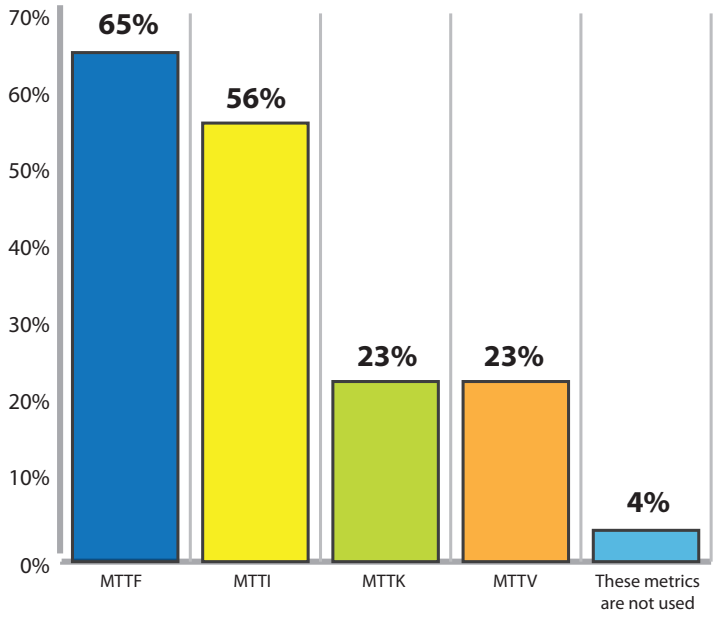
In this study, we asked respondents to confirm if they are using certain time-dependent operational metrics to measure incident response. These are:

- Mean time to identify (MTTI) or detect that an incident has occurred
- Mean time to know (MTTK) the root cause of an incident
- Mean time to fix (MTTF) a situation and restore service
- Mean time to verify (MTTV) and confirm the satisfactory resolution with the parties affected

Figure 7 shows that the most popular metrics are those that track the amount of time it took to resolve an incident and restore service (mean time to fix, used by 65 percent of respondents), followed by those that track the amount of time it took to identify an incident in the first place (mean time to identify, used by 56 percent of respondents).

FIGURE 7. Metrics used to determine incident response effectiveness

More than one response permitted



MTTK and MTTV are also valuable metrics that should be used more frequently.

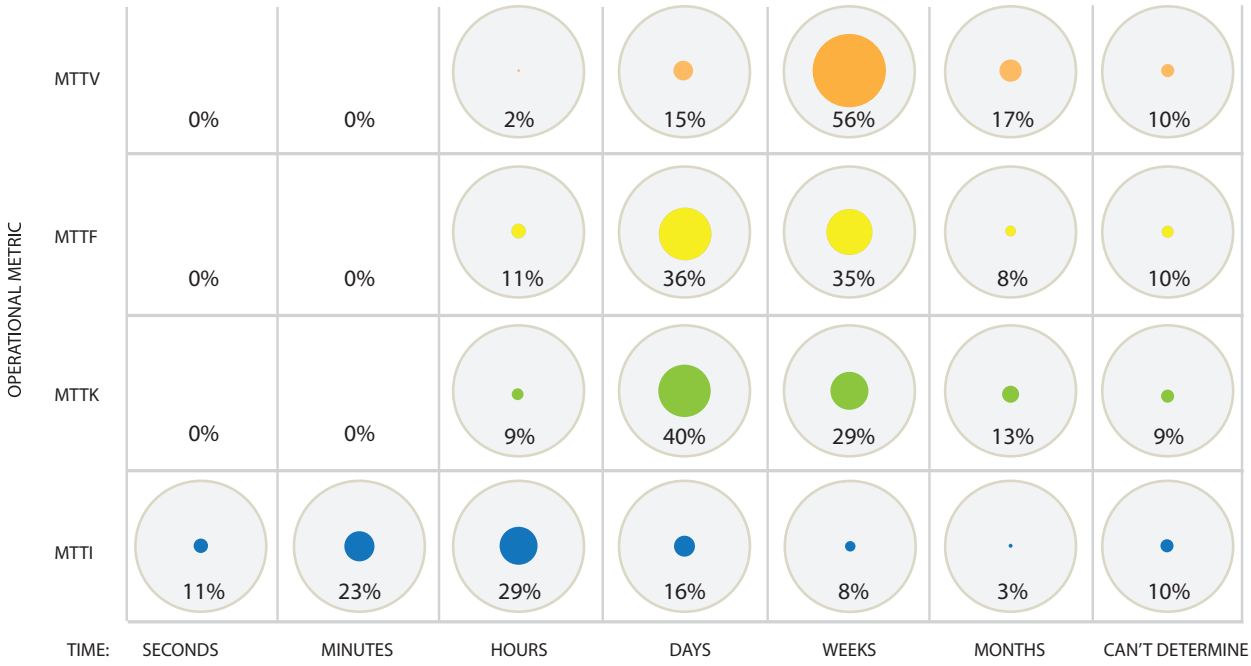
Improvements to an incident response team's toolsets and procedures can have a big impact on mean time to know. It is therefore beneficial to measure MTTK so that you can determine the impact of these improvements. Efficiency improvements will also impact the overall mean time to fix, if the organization is tracking that metric from the moment that the incident is identified.

Metrics that track the amount of time needed to verify that resolution of the incident was completed are also not used by many organizations. It is possible that many organizations don't have a separate verification step as part of their incident response process. Independent verification can be a helpful checkpoint when responding to a security breach, as a second set of eyes may identify an aspect of the compromise that was missed on the first pass. This is particularly important with sophisticated attackers who may leave behind very few traces of their activity.

We asked our survey respondents to tell us how long it took, on average, to identify a security incident in their network, determine the root cause, restore service and verify resolution. As shown in Figure 8, the majority of respondents said they could identify an incident within hours. In contrast, the entire incident resolution process can take weeks or months to complete.

FIGURE 8. How long it takes to respond

Approximate average MTTI, MTTK, MTTF and MTTV experienced by organizations in recent incidents

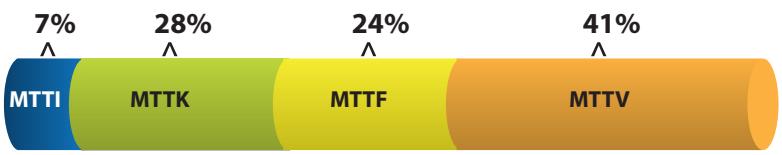


A key takeaway from these data points is that identification of a security incident is only a small part of the overall process of handling that incident.

It can take far longer to understand the incident, address it, and verify that it has been addressed than it takes to simply identify that it has occurred. The total time to get from compromise through the whole incident response process can take nearly a month on average. This suggests that business process improvements that reduce the amount of time that it takes to understand a security incident, restore infected computer systems, and verify that a breach has been addressed can have a significant impact on the overall cost of a breach. Figure 9 shows the breakdown of time spent by our respondents on each step of the incident resolution process over the course of a month.

FIGURE 9. Deconstruction of operational metric factors in incident response

Length of response time compared as percentage of hours



Do we really identify security incidents within hours?

OUR SURVEY RESPONDENTS were significantly more optimistic about the mean time to identify a security incident than the data provided by two other popular studies of computer security issues – the Verizon Data Breach Investigations Report and the Mandiant M-Trends Report. Both of those studies determined that it can take months, or even years, to identify that a breach has occurred, whereas our respondents claimed that they could do so within a matter of hours.

The most obvious explanation for this discrepancy is that our respondents may be referring to a broader cross-section of security incidents than those covered by the two aforementioned reports. Our respondents handle a variety of computer security incidents, from simple malware infections on desktops to complicated investigations of sophisticated, targeted attacks. The bulk of incidents likely consist of the former type.

The incidents covered by the Verizon and Mandiant reports were significant enough to warrant the involvement of an outside consulting firm, and in some cases, law enforcement. This factor may skew the results seen by those studies toward incidents that are more significant in scope and harder to detect.

However, it is also possible that our respondents suffer from unreasonable confidence in their own effectiveness at detecting breaches, which is not in line with reality. The data supporting the two aforementioned studies is accumulated from real incident reports and is therefore fact driven. The responses to our survey are the opinions of IT professionals and therefore reflect the perception rather than the facts. A large gap between perception and reality could indicate a significant cultural blind spot in IT security, and this subject is certainly worthy of further study.

Incident Response Team Practices

IN ADDITION TO asking about metrics, our survey asked respondents about a number of qualitative aspects of their incident response programs. These qualitative questions provide some indication of the maturity and readiness level of CSIRTs.

Many organizations are not assessing the readiness of their incident response teams on an ongoing basis.

A computer security incident response team is an organization that is tasked with jumping into action in order to address an emergency situation that can occur at any time. Unless there is a natural cadence of regular security incidents that provide constant feedback to the team regarding their responsiveness, it is useful to assess readiness through exercises. This is particularly true if many of the members of your team are not devoted to incident response on a full-time basis, and may need to be pulled off of other projects when an emergency occurs.

Forty-seven percent of our respondents either do not assess the readiness of their incident response teams or do not do so on a regular basis. On the other hand, 35 percent do so on a quarterly or ongoing basis, which indicates a high level of organizational maturity and preparedness.

Many incident response teams lack defined rules of engagement.

When computer security incidents occur, it is important to empower incident responders to act with autonomy. It is often necessary for responders to interfere with computer systems that are part of operational business processes, but may have been compromised by an attacker.

Incident response teams need to be able to gain rapid access to these compromised systems and they may need to pull those systems off of computer networks. Complex management approval requirements and resistance from business process owners can significantly delay incident response and increase the overall cost of the incident to the business. Only 45 percent of our respondents indicated that their incident response teams have clearly defined rules of engagement that enable them to operate with autonomy in the event of an incident.

Few organizations have a pre-defined public relations and analyst relations plan that they can put into motion in the event of a material data loss that needs to be publicly disclosed.

One of the most significant negative consequences associated with security breaches is the impact that they can have on the victim organization's reputation. In the event of a material exposure of customer data, it may be necessary for the organization to disclose facts about the breach to the general public. Organizations that can credibly and professionally communicate with the public about the nature of the breach and the steps that they are taking to address it have the opportunity to make the best of a difficult situation.

Unfortunately, only 23 percent of our respondents indicated that they have a defined PR and analyst relations plan in place. This is a surprisingly small percentage and indicates an area that deserves more focus from information security professionals. Public disclosure of information about a security breach involves difficult decisions regarding whether or not to disclose, what information to publish, where that information will be communicated, and who needs to be involved. Often, determinations need to be made regarding whether or not customer data was compromised, what legal and contractual obligations are invoked by the incident, and what the organization's strategy is moving forward.

Only 23%

of respondents indicated they have a defined PR and analyst relations plan in place.

The parameters for making these decisions should not be chosen on the fly in the midst of responding to an incident. Any organization with sensitive information should take the time to identify stakeholders regarding public disclosure and build processes and communications channels well in advance of a situation in which they are needed.

Few organizations have a multi-disciplinary insider threat management program.

Sometimes, the computer security incident that is being responded to is not an attack from the outside, but a crime committed by one of the organization's own employees. In these situations, a similar technical investigative process may be useful, but the right way to detect and manage these incidents differs significantly from situations that involve remote network compromises.

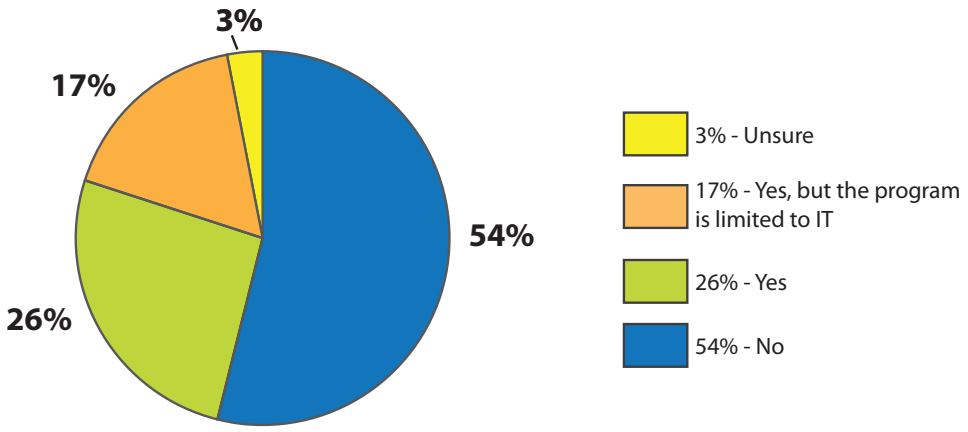
Only 26 percent of respondents indicated that a multi-disciplinary insider threat management program was in place in their organization. This is another area that deserves more focus from IT professionals. Notably, 17 percent of respondents indicated that they did have an insider threat program, but it was limited to IT and was not coordinated with human resources and the corporate legal department.

All too often, the insider threat is viewed by organizations as a computer security problem, and these problems are seen as technical issues to be dealt with exclusively by the IT department. In fact, insider threat is a categorically different problem, because in this case the attacker is an employee of the organization, and the relationship between the employee and the organization plays a significant role. In order to be effective, insider threat management programs need to reach across the organization, both to detect potential incidents and to manage the consequences when they occur.

Only 26%

of respondents indicated that a multi-disciplinary insider threat management program was in place in their organization.

FIGURE 10. Does your organization have a defined insider threat management program that involves cooperation among multi-disciplinary areas of the organization such as human resources, IT and legal?



Most organizations are not sharing threat intelligence and indicators.

The final step of an effective incident investigation is to collect what has been learned about the security deficiencies that the organization has, as well as the nature of the attacker, and put that information to use protecting the organization from future attacks. This is the heart of the reason that effective incident response can help protect the organization against future attacks, because the organization learns through this process how to better defend itself.

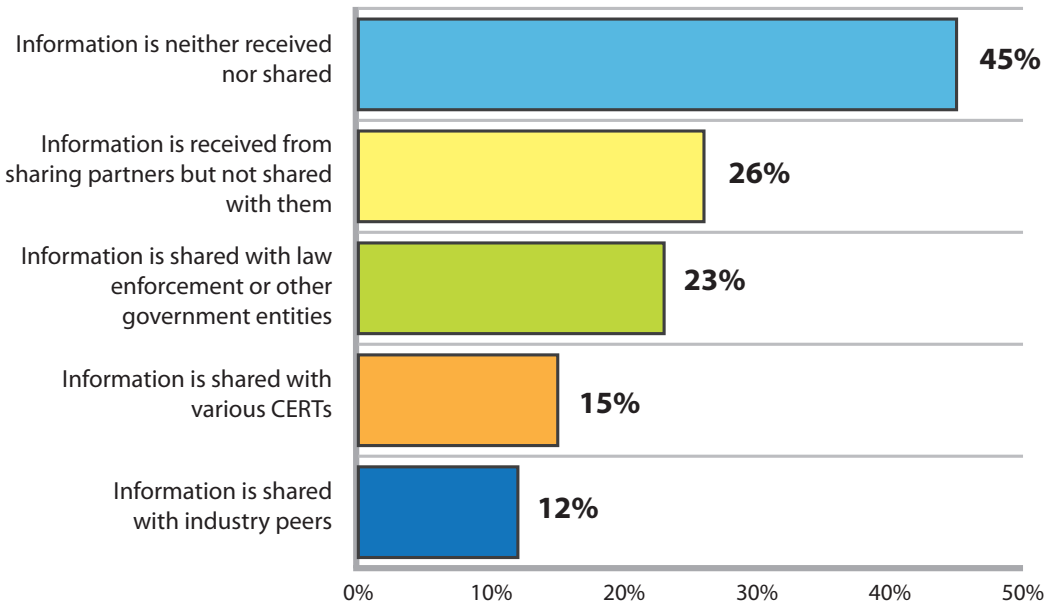
It is even better if the organization can share what it has learned with other organizations so that they can benefit as well. Unfortunately, the majority of organizations are not engaged in these follow-through efforts.

Fifty-four percent of our survey respondents indicated that their incident investigations do not result in the production of indicators that can be used to defend the organization against future attacks. Even if these indicators are produced, they are often not being shared. Forty-five percent of respondents indicated that they neither share threat intelligence with other organizations nor do they receive it. Another 26 percent indicated that they receive information but they do not share it.

As shown in Figure 11, if information is shared, it is most likely with law enforcement, but not industry peers. Commercial enterprises have a great deal to gain by sharing threat indicators with each other, and very little to lose. Hopefully this is an area in which we will see further improvement in the future.

FIGURE 11. Do organizations share threat indicators with other entities?

More than one response permitted



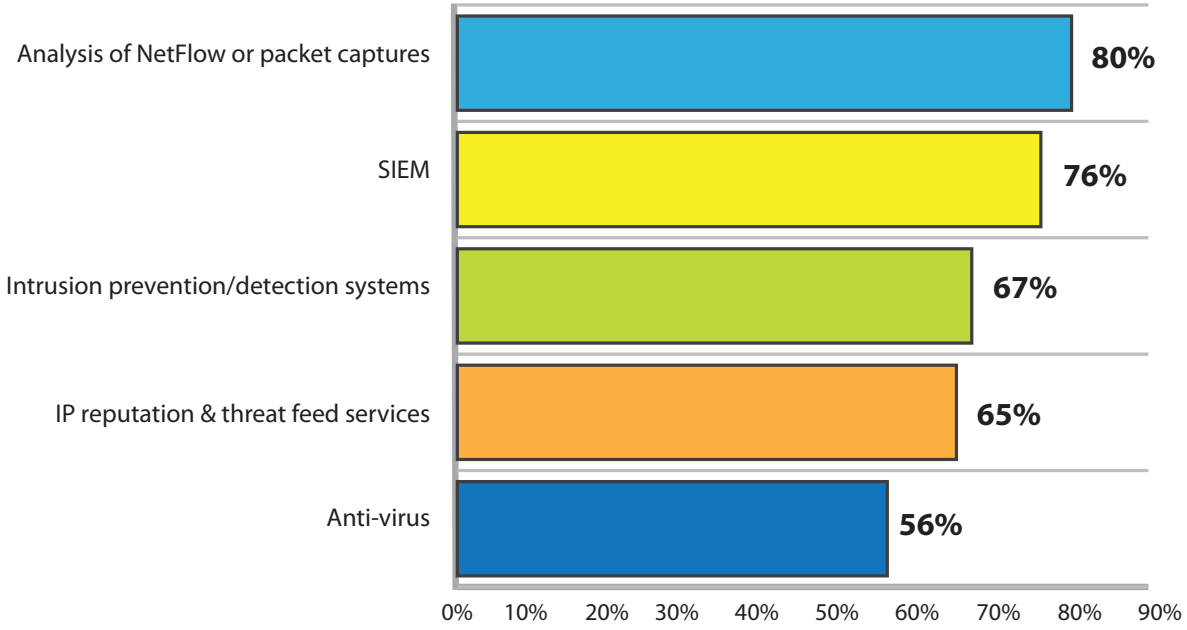
Incident Response Tools & Technologies

Technologies that collect audit trails of activity are the most effective tools for detecting attacks.

We asked our respondents to tell us what tools are most effective at detecting security breaches. The results are shown in Figure 12. Interestingly, the two most popular responses were tools that store audit trails of network- and system-level activity, rather than automated detection tools. Collections of NetFlow, packet captures and Syslog become a source of truth for an incident investigator that can enable the investigator to rewind the clock, whereas most automated detection tools are focused on what's happening in real time.

FIGURE 12. Most effective security tools for detecting security breaches

Very effective & effective responses combined



We also asked our respondents to provide information about their use of four common forensic audit trails – Syslog, NetFlow, packet capture and hard drive images. We asked respondents how widespread their deployment of these technologies is and how much history they store.

Collection of log information into a SEM or SIEM system

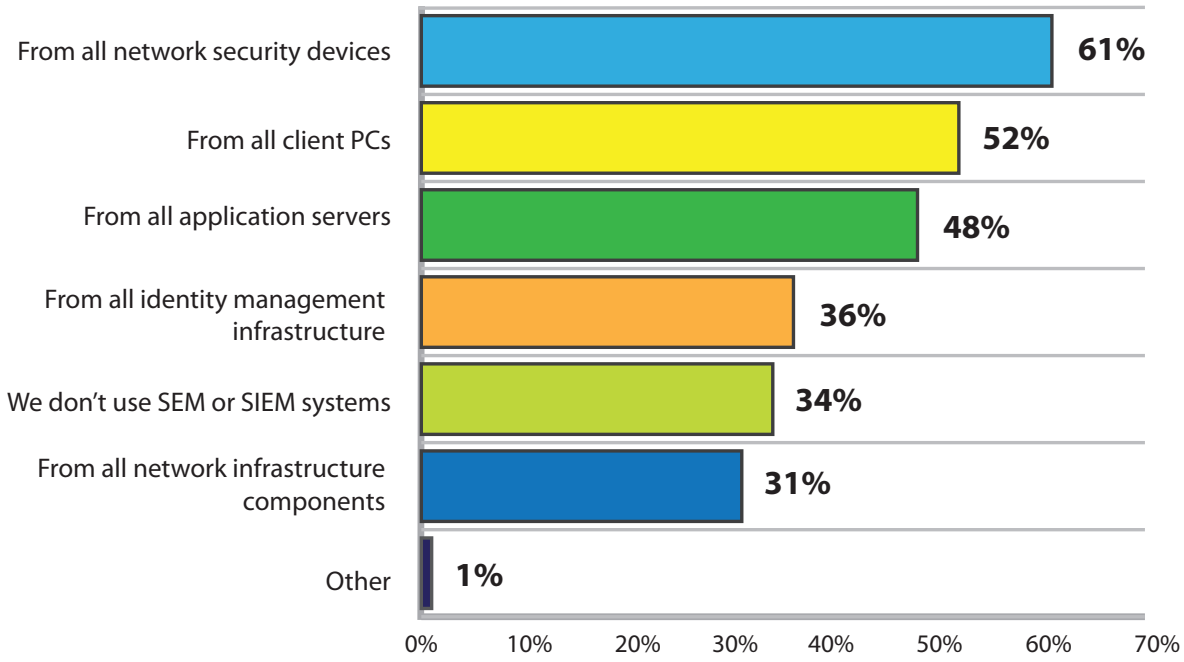
System logs are the first thing that many people think of when they think of forensic audit trails. They are produced by a wide range of client and server software and operating systems, as well as network and security devices.

Figure 13 reveals that 61 percent of respondents say their organization collects log information from network security devices (such as firewalls, IPS, etc.). More than half claimed to collect logs from all client PCs. Such system logs are most often kept for a month (according to 49 percent of respondents).

However, like all things, Syslog has limitations. You have to enable the collection of logs from each endpoint, so in many environments Syslog coverage is incomplete, and once a computer has been compromised, it's not possible to trust the logs coming from that device anymore. So Syslog is critical, but it can't tell you everything.

FIGURE 13. Methods for collecting log information for a SEM or SIEM system

More than one response permitted



Collection and storage of NetFlow

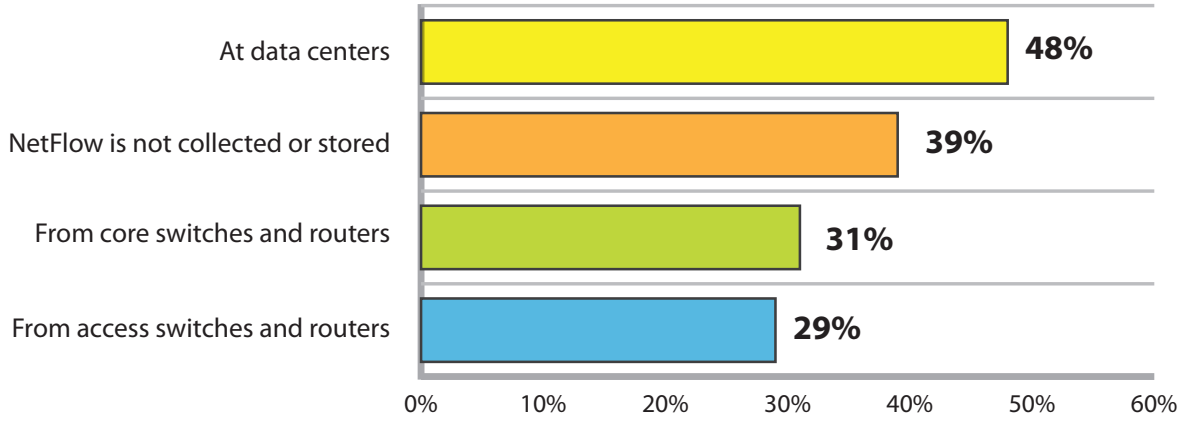
NetFlow is a family of standard protocols spoken by a wide variety of popular network equipment. It provides a record of each connection that occurs over a network, including the 'to' and 'from' addresses, port numbers and the amount of data transferred.

Although most NetFlow records do not include the content of communications, they are small, which makes them relatively inexpensive to store for long periods of time. They are also relatively inexpensive to collect throughout the network, because they can be obtained natively from a variety of network infrastructure devices without installing dedicated probes.

Figure 14 shows that NetFlow is most often collected at data centers. About a third of organizations are collecting NetFlow from access switches. Collecting NetFlow from access switches can provide a more complete picture of what has happened on a network than collecting from data centers alone, including records of traffic moving between different endpoints. Records of traffic streams between endpoint systems can help a forensic analyst determine how an attack spread within an internal network. Our respondents commonly store NetFlow for a month or more (43 percent), although many are only storing it for a week (37 percent).

FIGURE 14. How NetFlow is collected and stored

More than one response permitted



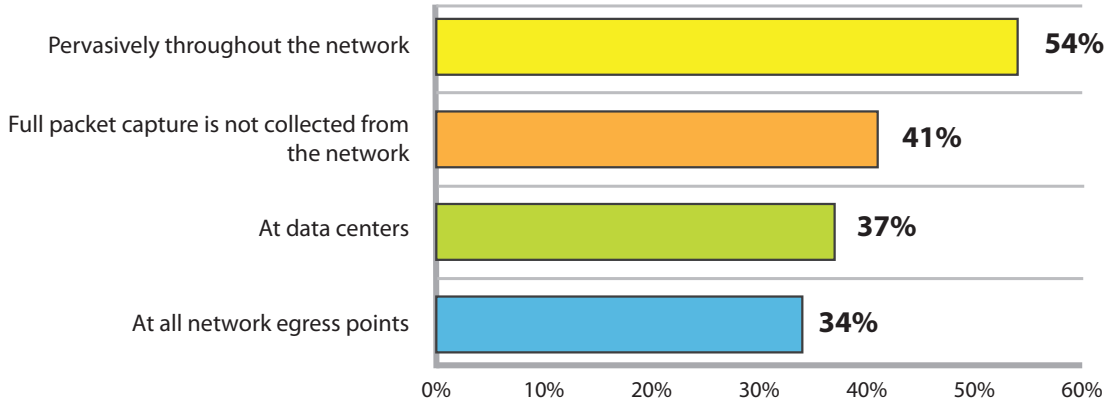
Collection of full packet capture

Modern packet capture appliances can collect a record of the full content of every communication that occurred over the network, and store that content for long periods of time. However, it can be very expensive to store all of this data, requiring signifigant storage capacity. Packet capture does, however, provide a comprehensive audit trail for the forensic analyst. A week's worth of full packet capture was the most common amount stored by our respondents (48 percent), although many claimed to be storing full packet capture for a month or more (34 percent).

We were surprised to see so many respondents indicate that they are collecting packet captures "pervasively throughout the network." It is difficult to collect packet captures everywhere in a network because of the need to install dedicated capture collection appliances at each collection point. What is telling is that some respondents who picked "pervasively throughout the network" also selected "at data centers" or "at all network egress points," whereas others did not. It is therefore our opinion that many respondents who selected "pervasively" have packet capture occurring at a variety of locations throughout their network, but do not have comprehensive coverage of all internal communications.

FIGURE 15. Where full packet capture is collected from the network

More than one response permitted



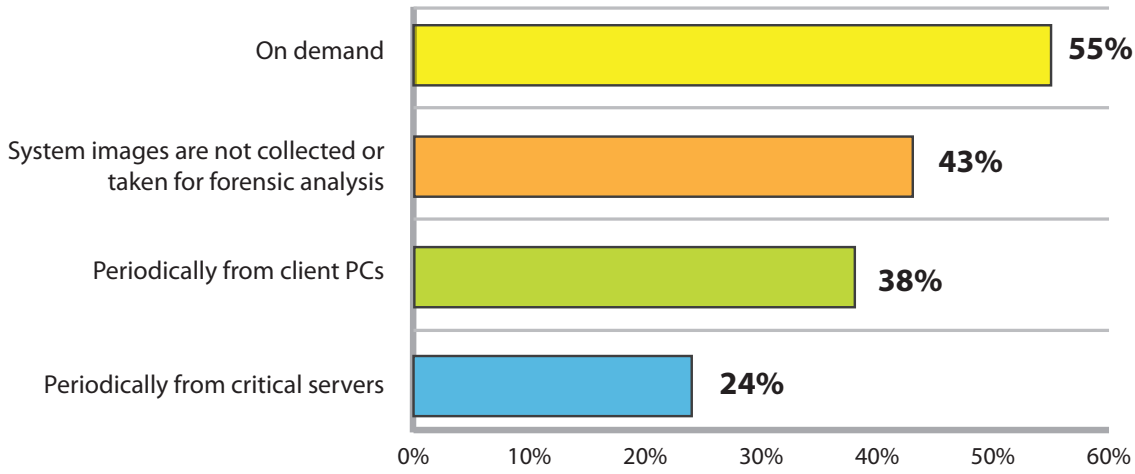
System images for forensic analysis

An image of a computer hard drive can capture the state of that computer at a particular time. These images are important for forensic analysts both to preserve evidence on the computer and to provide a way to analyze it. System images for forensic analysis are typically taken on demand, according to 55 percent of respondents (see figure 16).

Periodic collection of images can be more valuable because it provides a way for the analyst to recover the state that a computer might have been in earlier on during an incident, and retrieve data that an attack might have destroyed. A large number of respondents (43 percent) did not collect or take system images for forensic analysis at all.

FIGURE 16. How system images are taken for forensic analysis

More than one response permitted



Ultimately, each of these technologies have their place in an incident responder's toolset. Each creates an audit trail that provides different pieces of the puzzle of what was happening while the network was infected.

Management Visibility into Cyber Threats

Communication about potential cyber-attacks or threats posed against the organization often stays in IT management and little filters throughout the enterprise.

Only 24 percent of respondents say that frequent threat briefings are disseminated broadly within the organization and only 20 percent say this information reaches executives (see figure 17). The functions or departments involved in the incident response process are similarly limited to IT, legal and compliance followed by human resources (see figure 18). Executive management and the board of directors are seldom engaged.

There are a variety of reasons why executive management teams are not being briefed on the computer security threats faced by their organizations One reason may be that IT management doesn't like sharing bad news with executives, but it is also possible that executives view cyber threat information as being too technical and domain-specific for their use.

Regardless, if executives are in the dark about the nature of the computer security challenges that organizations face, then they are unlikely to provide adequate management support and funding for cyber security efforts, and they may feel blind-sided if a significant breach or service outage occurs as a result of a successful attack. Furthermore, many cyber security threats, such as spear phishing, directly target executive managers and members of the Board of Directors. These leaders may need to be informed about these threats in order to adequately protect themselves.

FIGURE 17. Frequency of cyber threat briefings to various functions

Very frequently and frequently responses combined

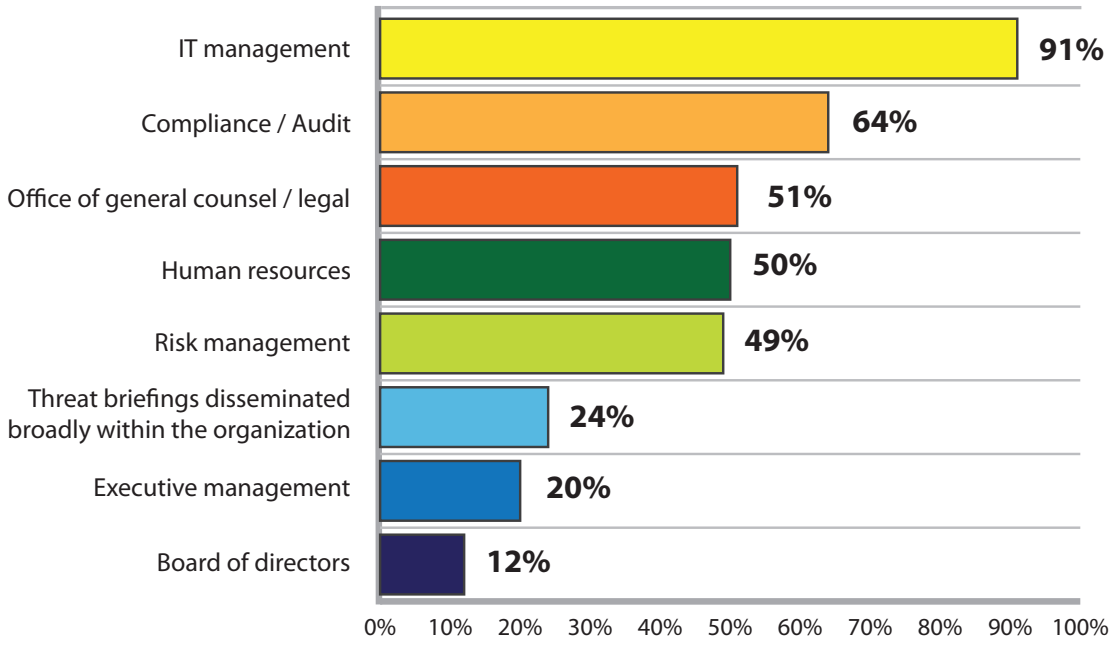
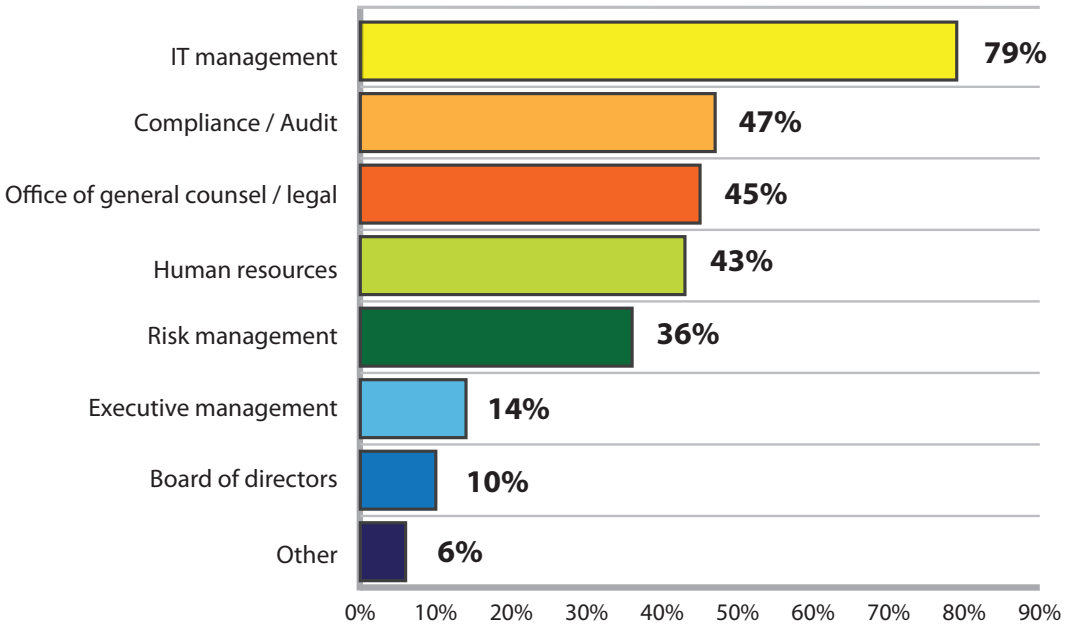


FIGURE 18. Functions or departments involved in the incident response process

More than one response permitted



Conclusion & Recommendations

Our survey respondents agree that it is possible for organizations to protect themselves more effectively against the threats that they face on the Internet. They also agree that greater investment in incident response capabilities is the best thing that their organizations could be doing to protect themselves.

However, most organizations don't seem to be making those investments. Every organization, no matter how small, should have a designated person who is responsible for computer security incident response. In addition, every organization should be asking itself three key questions about its incident response capabilities:

Are we prepared to handle the incidents that our organization might face?

Our research has found that many incident response teams appear to be under funded. They may lack the tools and forensic audit trails that they need to property investigate incidents. They may not have the staff that they require, or access to consultants who can augment full-time staff in emergencies. They may not have engaged in basic incident planning, such as crafting a PR and analyst relations plan to execute in the event of a breach. They may not be testing their readiness on a regular basis.

Ask yourself, what is my efficiency of response? What are the kinds of attacks that my organization might expect and what is going to happen when those attacks occur? Who is responsible for responding, and do they have everything that they need to respond effectively? Can they operate with autonomy in the event of an incident and take action to mitigate it? Also ask yourself, do we learn things from breaches that allow us to better protect the organization in the future? Are we sharing what we've learned?

Are we measuring the effectiveness of our incident response efforts?

If your organization isn't measuring incident response, you don't really understand the cost of the incidents that you are experiencing. Ultimately, every computer security program has to do with reducing the cost of breaches and incidents. The amount of time and effort required to respond to incidents, understand them, and mitigate them is part of that cost, as is the operational impact, downtime, loss of intellectual property, reputational impact and other negative consequences that breaches have on the organization.

A properly equipped and trained incident response team can contain breaches more rapidly, reduce their impact on the organization, and apply what they've learned to protect the organization against future attacks. In order to justify the expense of training and equipping incident responders, you've got to be able to measure their effectiveness, and you've got to incorporate those metrics into an overall understanding of the financial impact of the organization's computer security program.

Recommendations

- **Make** it a priority to build an incident response team consisting of experienced, full-time members
- **Assess** the readiness of incident response team members on an ongoing basis
- **Create** clearly defined rules of engagement for the incident response team
- **Have** meaningful operational metrics to gauge the overall effectiveness of incident response
- **Translate** the results of these measures into user-friendly business communications
- **Involve** multi-disciplinary areas of the organization in the incident response process
- **Invest** in technologies that support the collection of information to identify potential threats
- **Consider** sharing threat indicators with third-party organizations to foster collaboration

Are we communicating effectively with upper management about the threats that our organization faces?

Without management support and sufficient resources, companies can face an uphill battle in the war against cyber criminals and malicious insiders. Our research indicates that organizations are not communicating with business leaders about computer security threats. Whether this is because they are afraid to admit the realities to the people that they work for, or because they don't know how to articulate those realities in dollars and cents terms that are relevant to business decision makers, the consequences are the same.

Computer security programs in general and incident response teams specifically may be under funded. It is not only important that organizations track the incidents they are experiencing; it's also important to relate those incidents to the financial bottom line of the organization, and convey that information to business leaders. Computer security needs to be a boardroom discussion, before the organization is in the headlines, and not after.

If you can answer all three of these questions affirmatively, our research indicates that your organization is better positioned than most that we surveyed to address sophisticated cyber-attacks. The computer security threat landscape presents more challenges every year, but with the right incident response capabilities, you'll be ready to face them.

Methodology

A random sampling frame of 20,446 experienced IT and IT security practitioners located in all regions of the United States and United Kingdom were selected as participants in this survey. To ensure knowledgeable responses, all participants in this research have some level of familiarity and involvement with their organization's CSIRT activities.

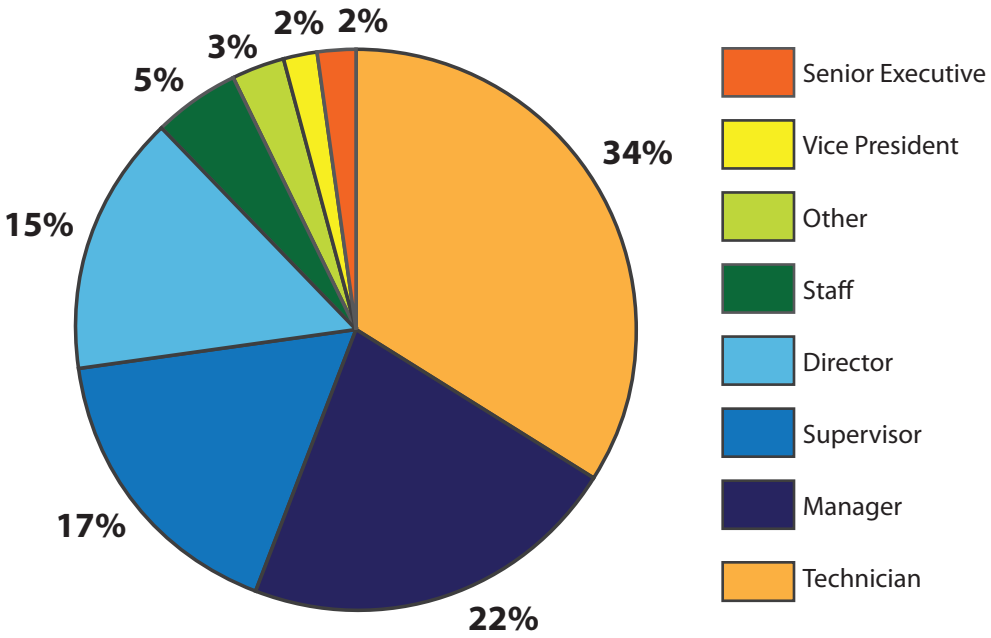
As shown in Table 1, 793 respondents completed the survey. Screening and reliability checks removed 119 surveys. The final sample was 674 surveys (or a 3.3 percent response rate).

TABLE 1. Sample response

	Freq	Pct%
Sampling frame	20,446	100%
Total returns	793	3.9%
Rejected and screened surveys	119	0.6%
Final sample	674	3.3%

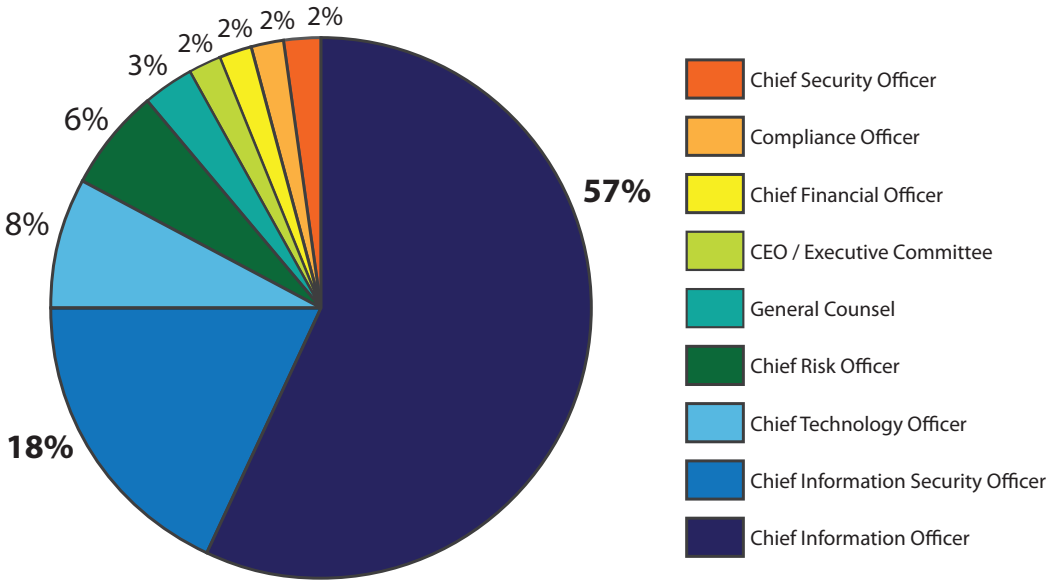
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, 58 percent of respondents are at or above the supervisory levels.

PIE CHART 1. Current position within the organization



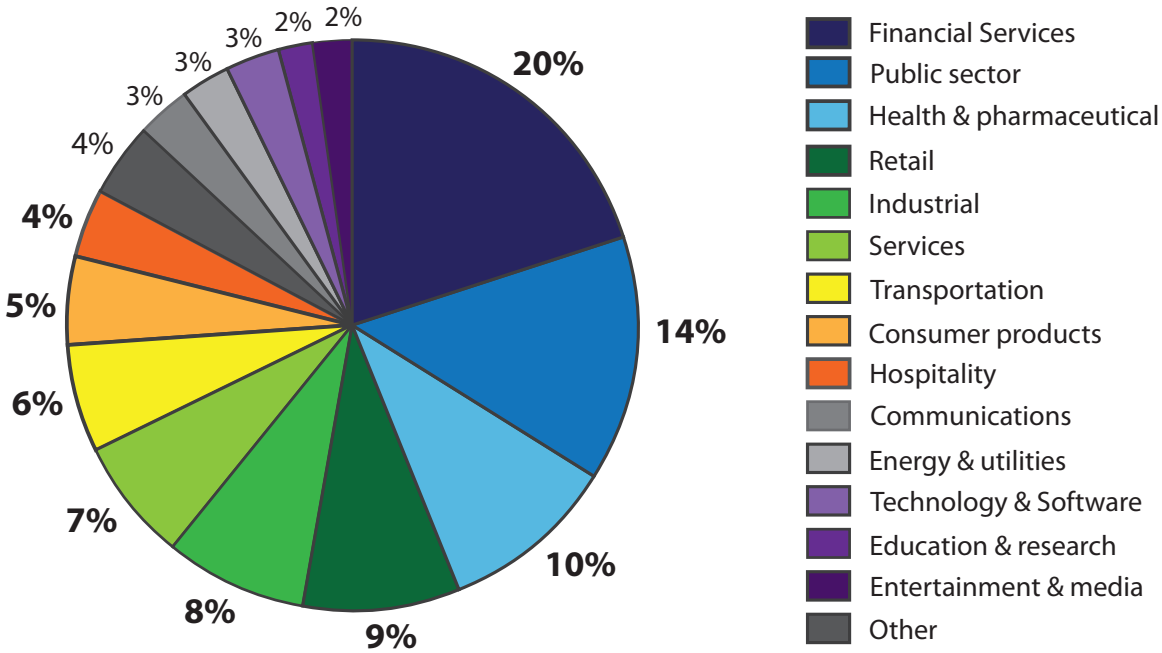
Pie Chart 2 reports the primary person to which the respondent or their immediate supervisor reports. Fifty-seven percent report to the CIO and 18 percent report to the CISO.

PIE CHART 2. The primary person you or your immediate supervisor reports to within the organization



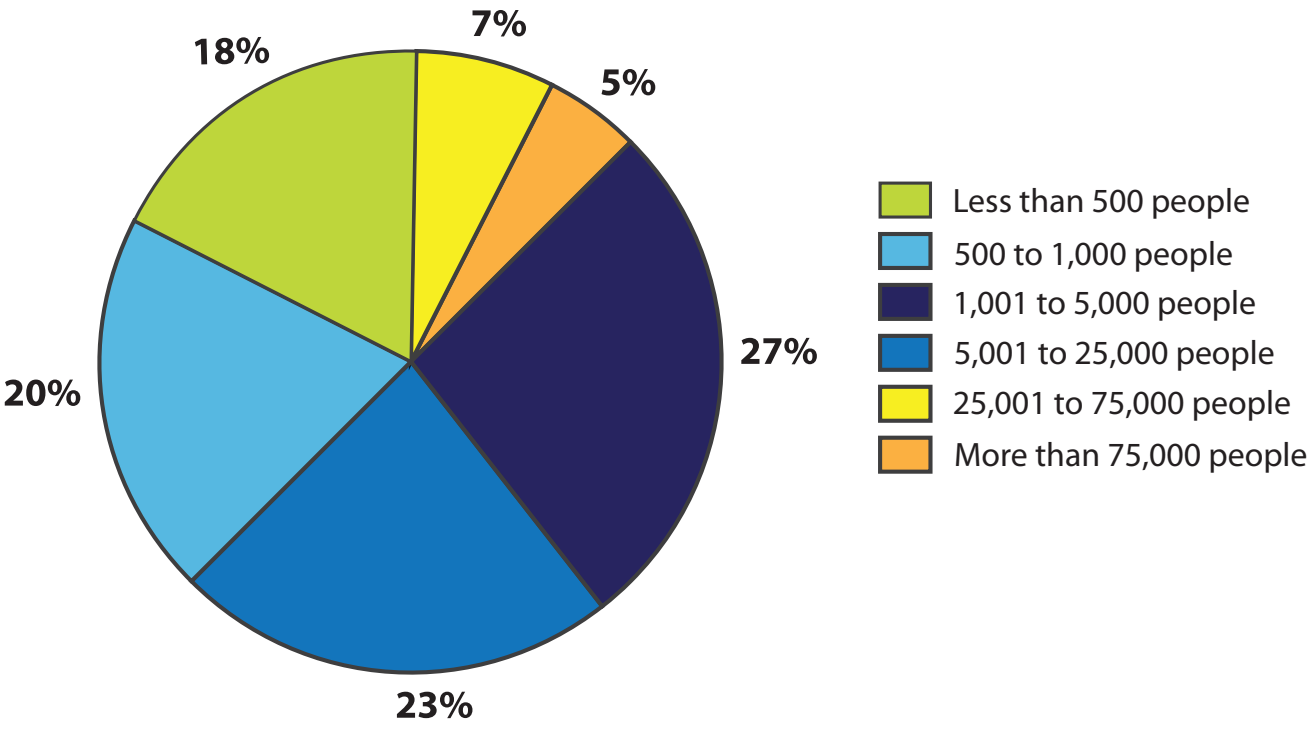
Pie Chart 3 reports the industry segments of respondents' organizations. This chart identifies financial services (20 percent) as the largest segment, followed by government (14 percent) and healthcare at 10 percent.

PIE CHART 3. Industry distribution of respondents' organizations



As shown in Pie chart 4, 62 percent of respondents are from organizations with a global head count of 1,000 or more employees.

PIE CHART 4. Worldwide head count of the organization



There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- **Non-response bias:** The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.
- **Sampling-frame bias:** The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.
- **Self-reported results:** The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in August 2013.

Sample Response	Frequency
Total sampling frame	20,446
Total returns	793
Total rejections and screened surveys	119
Final sample	674
Response rate	3.3%
Sample weights	**100%**

Part 1: Screening questions

S1. How familiar are you with your organization's CSIRT activities?

Very familiar	41%
Familiar	34%
Somewhat familiar	25%
Not familiar (stop)	0%
Total	**100%**

S2. Are you involved in your organization's CSIRT?

Significant involvement	53%
Some involvement	47%
No involvement (stop)	0%
Total	**100%**

Part 2: Survey questions

Q1. In the past 24 months, how many security incidents or breaches did your organization experience?

None	32%
One	31%
2 to 5	19%
6 to 10	13%
More than 10	5%
Total	**100%**

Q2. Do you anticipate that your organization will experience a material security breach sometime in the near future?

Yes, within the next 3 months	30%
Yes, within the next 6 months	16%
Yes, within the next year	11%
Yes, in more than one year	12%
No	31%
Total	**100%**

Q3. In your opinion, how can your organization best mitigate future security breaches? Please select your top three choices.

Improved security policies and compliance practices	11%
More effective employee training	15%
Higher quality professional staffing	29%
Improved vulnerability audits and assessments	44%
Improved patch management process	36%
Advanced preventative technologies	20%
Outsourced or managed security services	13%
Threat intelligence or IP reputation services	62%
Better incident response capabilities	68%
Other (please specify)	2%
Total	**300%**

Q4. Please rate the following statement: The right investments in people, process and technologies would allow my organization to mitigate all future security breaches.

Strongly agree & Agree	81%

Q5. Does your organization have a fully functional CSIRT in place today?

Yes	66%
No (Go to Q12)	34%
Total	**100%**

Q6. How long has a formal CSIRT program existed within your organization?

Less than 1 year	18%
1 to 2 years	22%
3 to 5 years	36%
More than 5 years	24%
Total	**100%**

Q7. How many security analysts/practitioners (team members) are assigned to your organization's CSIRT?

None	12%
One	16%
2 to 5	44%
6 to 10	23%
More than 10	5%
Total	**100%**

Q8. How many team members are fully dedicated to CSIRT?

None	45%
One	28%
2 to 5	14%
6 to 10	11%
More than 10	2%
Total	**100%**

Q9. Approximately, what is the average relevant experience of CSIRT members (in years)?

Less than 2 years	3%
2 to 5 years	7%
6 to 10 years	36%
More than 10 years	54%
Total	**100%**

Q10. What percentage of CSIRT members hold relevant certifications in IT or cyber security (such as the CISSP, CISM, CISA and others)?

None	3%
Less than 25%	9%
25 to 50%	12%
51 to 75%	36%
76 to 100%	40%
Total	**100%**

Q11. Do CSIRT members undergo specialized training on an ongoing basis?

Yes	48%
No	50%
Unsure	2%
Total	**100%**

Q12. What percentage of your organization's security budget is allocated to incident response? Please include personnel, services and technology costs/investments in your estimate. Your best guess is welcome.

Less than 10%	50%
10% to 20%	31%
21% to 30%	11%
31% to 40%	5%
41% to 50%	2%
More than 50%	1%
Total	**100%**

Q13. How has this percentage changed over the past 24 months?

Increased	34%
Decreased	18%
Stayed the same	45%
Cannot determine	3%
Total	**100%**

Q14. Do you have a retainer or master service agreement with a third-party consulting firm that can assist you and your organization with incident response?

Yes	35%
No	60%
Unsure	5%
Total	**100%**

Q15. [If yes to Q14] What best describes the third-party service provider selected by your organization in the event of an incident?

Global audit or consulting firm	15%
Regional or local audit or consulting firm	6%
Forensics and investigative firm	46%
Risk management firm	9%
Law firm	24%
Other (please specify)	0%
Total	**100%**

Q16. What best describes how this service provider (vendor) is utilized by your organization?

As a primary first responder to security incidents	10%
To augment the skill set of your incident response team	42%
To augment the capacity of your incident response team during crisis situations	31%
All of the above	16%
Other (please specify)	1%
Total	**100%**

Q17. Does your organization have meaningful operational metrics to measure the overall effectiveness of incident response activities?

Yes	46%
No	50%
Unsure	4%
Total	**100%**

Q18. Does your organization have meaningful operational metrics to measure the speed at which incidents are being detected and contained?

Yes	42%
No	55%
Unsure	3%
Total	**100%**

Four time-dependant operational metrics defined as follows:

Mean time to identify (MTTI).
This is the time it takes to detect that an incident has occurred.

Mean time to know (MTTK).
This constitutes the time it takes to locate the root cause of an incident.

Mean time to fix (MTTF).
This is the time it takes for a responder to resolve a situation and ultimately restore service.

Mean time to verify (MTTV).
This is the time it takes to confirm the satisfactory resolution with the parties affected.

Q19. [Q18 = Yes] What time-dependent metrics does your organization use to determine the relative effectiveness of your organization's incident response process?

MTTI	56%
MTTK	23%
MTTF	65%
MTTV	23%
We don't utilize time-dependent operational metrics	4%
Total	171%

Q20. Please rank the four time-dependent metrics in terms of their relative difficulty in measuring. Here, 1 = most difficult and 4 = least difficult.

	Average rank
MTTI	2.98
MTTK	1.60
MTTF	1.55
MTTV	3.41

Q21. Approximately, what is an average MTTI experienced by your organization in recent incidents? Your best guess is welcome.

Within seconds	11%
Within minutes	23%
Within hours	29%
Within days	16%
Within weeks	8%
Within months	3%
Other (please specify)	0%
Cannot determine	10%
Total	100%

Q22. Approximately, what is an average MTTK experienced by your organization in recent incidents? Your best guess is welcome.

Within seconds	0%
Within minutes	0%
Within hours	9%
Within days	40%
Within weeks	29%
Within months	13%
Other (please specify)	0%
Cannot determine	9%
Total	100%

Q23. Approximately, what is an average MTTF experienced by your organization in recent incidents? Your best guess is welcome.

Within seconds	0%
Within minutes	0%
Within hours	11%
Within days	36%
Within weeks	35%
Within months	8%
Other (please specify)	0%
Cannot determine	10%
Total	**100%**

Q24. Approximately, what is an average MTTV experienced by organizations in recent incidents? Your best guess is welcome.

Within seconds	0%
Within minutes	0%
Within hours	2%
Within days	15%
Within weeks	56%
Within months	17%
Other (please specify)	0%
Cannot determine	10%
Total	**100%**

Q25. How does your organization collect log information for a SEM or SIEM system? Please select all that apply.

From all network security devices (such as Firewalls, IPS)	61%
From all application servers	48%
From all network infrastructure components	31%
From all identity management infrastructure	36%
From all client PCs	52%
We don't use SEM or SIEM systems	34%
Other (please specify)	1%
Total	**263%**

Q26. How many days of system logs does your organization retain/store?

None	0%
Less than 1 day	2%
About 1 day	8%
About 1 week	25%
About 1 month	49%
More than 1 month	16%
Other (please specify)	0%
Total	**100%**

Q27. Where does your organization collect full packet capture from the network? Full packet capture refers to the process of intercepting and logging all network (both header and payload) traffic.

At data centers	37%
At all network egress points	34%
Pervasively throughout the network	54%
Other (please specify)	0%
We don't collect full packet capture from the network (Go to Q.29)	41%
Total	**166%**

Q28. How many days of full packet capture is your organization storing?

None	0%
Less than 1 day	4%
About 1 day	14%
About 1 week	48%
About 1 month	25%
More than 1 month	9%
Other (please specify)	0%
Total	**100%**

Q29. How does your organization collect and store NetFlow? NetFlow is a network protocol for collecting IP traffic information and has become an industry standard for traffic monitoring.

At data centers	48%
From core switches and routers	31%
From access switches and routers	29%
Other (please specify)	0%
We don't collect and store NetFlow	39%
Total	**147%**

Q30. How many days of NetFlow does your organization store?

None	0%
Less than 1 day	5%
About 1 day	15%
About 1 week	37%
About 1 month	32%
More than 1 month	11%
Other (please specify)	0%
Total	**100%**

Q31. How does your organization take system images for forensic analysis?

On demand	55%
Periodically from critical servers	24%
Periodically from client PCs.	38%
Other (please specify)	0%
We don't collect take system images for forensic analysis	43%
Total	**160%**

Q32. Do your organization's incident investigations result in the production of threat indicators, which are then used to defend the organization from future attacks?

Yes	43%
No	54%
Unsure	3%
Total	**100%**

Q33. Does your organization share threat indicators with the following entities? Please check all that apply.

Various CERTs	15%
Law enforcement or other government entities	23%
Industry peers	12%
We receive information from sharing partners but we do not share information with them.	26%
We neither receive nor share any information	45%
Other (please specify)	0%
Total	**121%**

Q34. Are you sharing threat indicator information with the above-mentioned entities using standardized protocols? If so, please select all that apply.

TAXII/STIX/CybOX	43%
Open IOC	31%
Unstructured PDF or CSV	20%
Other (please specify)	6%
Total	**100%**

Q35. Does your organization's incident response team have clearly defined rules of engagement that enable them to act with autonomy in the event of a significant attack?

Yes	45%
No	51%
Unsure	4%
Total	**100%**

Q36. How frequently (and with whom) do you communicate about potential cyber-attacks or threats posed against your organization? Please use the following scale: 1 = very frequently, 2 = frequently, 3 = not frequently, 4 = none (no communication).

	Combined Very frequently & Frequently
IT management	91%
Executive management	20%
Board of directors	12%
Risk management	49%
Office of general counsel/legal	51%
Compliance/audit	64%
Human resources	50%
Threat briefings disseminated broadly within the organization	24%

Q37. What functions or departments are involved in the incident response process? Please select all that apply.

IT management	79%
Executive management	14%
Board of directors	10%
Risk management	36%
Office of general counsel/legal	45%
Compliance/audit	47%
Human resources	43%
Other (please specify)	6%
Total	**280%**

Q38. Does your organization have a defined insider threat management program that involves cooperation among multi-disciplinary areas of the organization such as human resources, IT and legal?

Yes	26%
Yes, but the program is limited to IT	17%
No	54%
Unsure	3%
Total	**100%**

Q39. Does your organization have a public relations and analyst relations plan in the event of a material breach that needs to be publicly disclosed?

Yes	23%
No	75%
Unsure	2%
Total	**100%**

Q40. What enabling security tools or solutions are most effective in helping your organization detect security breaches? Please rate each security tool using the following four-point effectiveness scale: 1 = very effective, 2 = effective, 3 = somewhat effective, 4 = not effective.	Combined Very effective & Effective
Intrusion prevention/detection systems	67%
Anti-virus	56%
Advanced malware detection systems	54%
Log Analysis	41%
SIEM	76%
Analysis of NetFlow or packet captures	80%
IP reputation and threat feed services	65%
Threat indicator information shared by industry peers	30%
Contact by law enforcement	27%
Reports of suspicious activity by end users	49%
Third-party verification and auditing services	44%

Q41. How frequently does your organization assess the readiness of your incident response teams (for instance, through tabletop exercises, red teams, or other means)?	
On an ongoing basis	21%
On a quarterly basis	14%
On a semi-annual basis	6%
On an annual basis	12%
Not on a regular schedule	29%
Readiness is not assessed	18%
Total	**100%**

Part 3: Your role and organization

D1. What organizational level best describes your current position?

Senior Executive	2%
Vice President	2%
Director	15%
Manager	22%
Supervisor	17%
Technician	34%
Staff	5%
Contractor/Consultant	2%
Other	1%
Total	**100%**

D2. Check the Primary Person you or your immediate supervisor reports to within the organization.

CEO/Executive Committee	2%
Chief Financial Officer	2%
General Counsel	3%
Chief Information Officer	57%
Chief Technology Officer	8%
Chief Information Security Officer	18%
Compliance Officer	2%
Chief Privacy Officer	0%
Human Resources VP	0%
Chief Security Officer	2%
Chief Risk Officer	6%
Other (please specify)	0%
Total	**100%**

D3. Total years of relevant experience

	Mean
Total years of IT or security experience	9.89
Total years in current position	5.67

D4. What industry best describes your organization's industry focus?

Agriculture & food services	1%
Communications	3%
Consumer products	5%
Defense	1%
Education & research	2%
Energy & utilities	3%
Entertainment & media	2%
Financial services	20%
Health & pharmaceutical	10%
Hospitality	4%
Industrial	8%
Public sector	14%
Retail	9%
Services	7%
Technology & software	3%
Transportation	6%
Other	2%
Total	**100%**

D5. Where are your employees located? (Check all that apply):

United States	86%
Canada	75%
UK/Europe	89%
Middle East & Africa	45%
Asia-Pacific	53%
Latin America (including Mexico)	49%

D6. What is the worldwide head count of your organization?

Less than 500 people	18%
500 to 1,000 people	20%
1,001 to 5,000 people	27%
5,001 to 25,000 people	23%
25,001 to 75,000 people	7%
More than 75,000 people	5%
Total	**100%**

For more information about this study

Visit Lancope at www.lancope.com
and follow on twitter @Lancope

Visit Ponemon Institute
at www.ponemon.org
and follow on twitter @PonemonPrivacy

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

Lancope®

Lancope, Inc. is a leading provider of network visibility and security intelligence to defend organizations against today's top threats. Delivering pervasive insight across distributed networks, Lancope improves incident response, streamlines forensic investigations and reduces enterprise risk. Lancope's security capabilities are continuously enhanced with threat intelligence from the StealthWatch® Labs research team and its business partners.

VISION TO SECURE, INTELLIGENCE TO PROTECT

IRv1-r007-01172014